

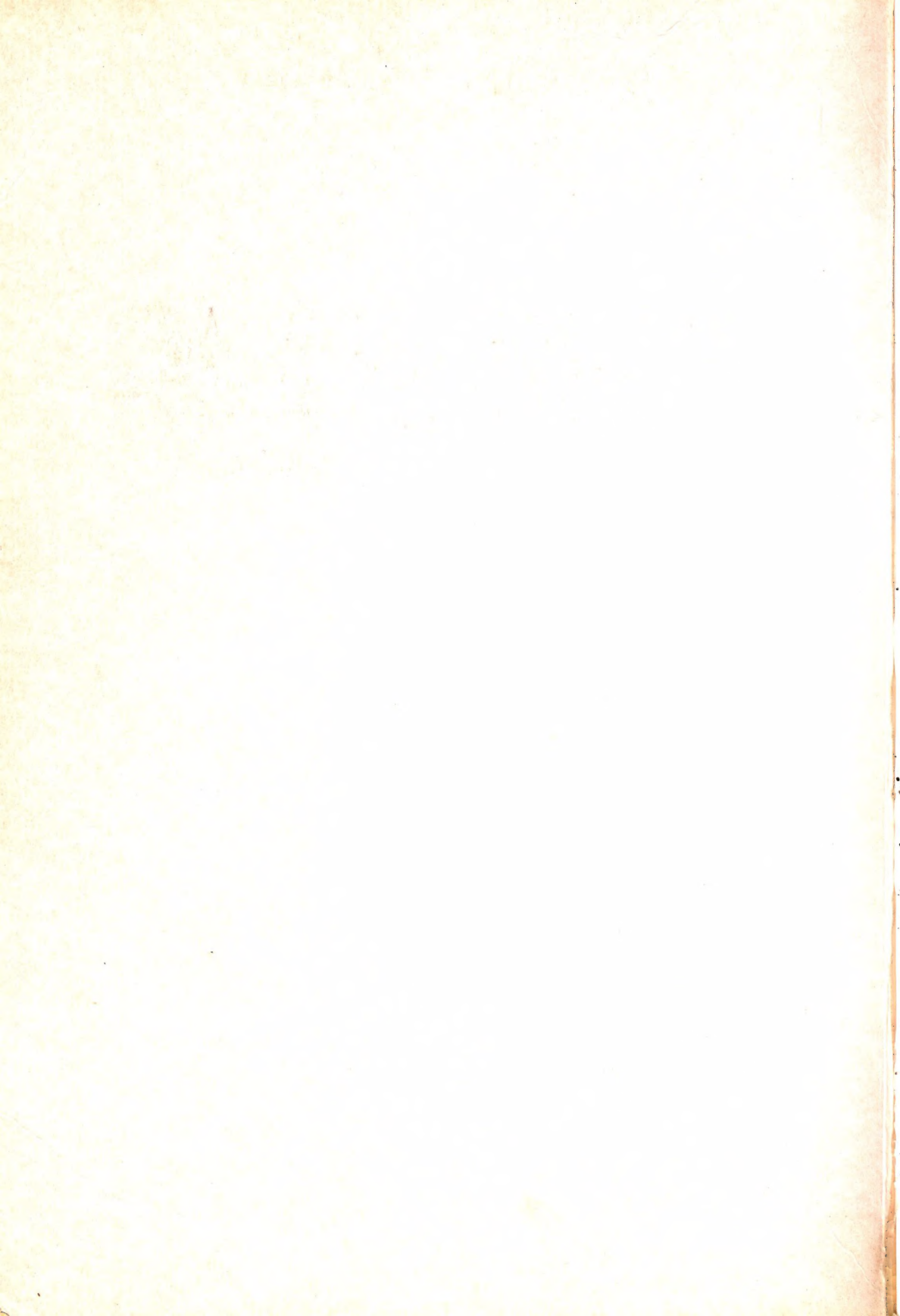
Федор Зубанов

WINDOWS NT

— выбор "профи"



 РУССКАЯ РЕДАКЦИЯ



Федор Зубанов

WINDOWS NT

– выбор "профи"

 **РУССКАЯ РЕДАКЦИЯ**

Федор Зубанов

- 391 Windows NT — выбор "профи". — М., Издательский отдел "Русская Редакция" ТОО "Channel Trading Ltd.", 1996 — 392 с.: ил.
ISBN 5—7502—0018—3

Основное внимание в книге уделяется вопросам планирования, установки, защиты и администрирования, обеспечивающих безотказную работу вычислительной системы. В частности, рассматриваются: доменная структура сетей Microsoft, учетные записи пользователей и групп, управление политикой ведения учетных записей, вопросы отказоустойчивой работы с дисками, кластерные технологии, файловые системы, безопасная работа в глобальных сетях и при подключении к Internet. Кроме того, описываются особенности новой, 4 версии Windows NT. Книга снабжена иллюстрациями, состоит из введения, 12 глав (включая приложения), словаря терминов и предметного указателя. Издание рассчитано на специалистов, занимающихся планированием, созданием и эксплуатацией компьютерных сетей под управлением операционной системы Microsoft Windows NT Server.

© Зубанов Ф. В., 1996

© Оформление и подготовка к изданию изд. отдела "Русская Редакция" ТОО "Channel Trading Ltd.", 1996

Microsoft, MS-DOS, Windows являются охраняемыми товарными знаками Microsoft Corporation, Windows NT является товарным знаком Microsoft Corporation. Все другие зарегистрированные товарные знаки и товарные знаки являются собственностью соответствующих фирм.

Введение	I
Основные свойства Windows NT	I
Приоритетная многозадачность	I
Встроенная сетевая поддержка	I
Защищенность	II
Многопоточность	II
Поддержка симметричной мультипроцессорной обработки	II
Поддержка широкого спектра компьютерных платформ	III
Возможность выполнения приложений, написанных для других операционных систем	III
Поддержка нескольких файловых систем	III
Знакомый интерфейс	III
Интеллектуальная программа установки	IV
Различие между версиями Windows NT	IV
Функции Windows NT Server	IV
Windows NT Server как файл-сервер	V
Windows NT Server как сервер печати	V
Windows NT Server как сервер приложений	V
Windows NT Server как сервер резервирования данных	VI
Windows NT Server как сервер удаленного доступа	VI
Windows NT Server как сервер связи сетей	VII
Главная проблема администрирования	VII
Об этой книге	VII
 I Служба каталогов Windows NT	 1
Сетевые модели: рабочие группы и домены	2
Модель рабочих групп	2
Доменная модель	2
Администрирование домена	3
Нагрузочная способность доменов	6
Доверительные отношения	7
Типы доверительных отношений	7
Типы доменных моделей	10

Однодоменная модель	10
Модель с одним мастер-доменом	11
Модель с несколькими мастер-доменами	14
Модель полностью доверительных отношений	16
Практическая реализация доменных моделей	17

Гибкость использования разных моделей доменов в организациях 18

Предприятия с несколькими независимыми направлениями производства	18
Крупные предприятия	19
Филиалы	20
Защищенные домены	20
Рекомендации по нагрузке доменов 22	
Требования к серверу при установлении доверительных отношений	23

II Планирование и установка системы 25

Планирование системы 26

Роль Windows NT Server в сети	26
Файл-сервер	27
Сервер печати	28
Сервер приложений	28
Сервер удаленного доступа	29
Сервер вспомогательных служб	29
Контроллер домена	30
Сервер взаимодействия с Netware	30
Выбор техники	31
Выбор необходимого объема оперативной памяти	33
Определение объема жесткого диска	35
Выбор файловой системы	36
Выбор процессора	36
Выбор сетевых протоколов	37
Планирование клиентских лицензий	39
Процедура установки 42	
Выбор способа установки	43
Неграфическая часть установки	44
Графическая часть установки	45
Установка Windows NT на большое число компьютеров	50

III Защита информации и система безопасности Windows NT	53
Защищенная система — уровень C2 и лучше	54
Уровень защиты C2 — определение требований	55
Сертификация Windows NT на уровень C2	55
Решение реальных проблем защиты	56
Обеспечение защиты в корпоративной системе	57
Поддержка системы безопасности корпорации	57
Модель безопасности Windows NT	58
Распорядитель локальной безопасности	59
Менеджер защиты учетных записей	59
Справочный монитор безопасности	61
Процесс регистрации	62
Предупреждение о легальности использования	64
Регистрация в Windows NT 4.0	65
<i>Настройка параметров удаленного доступа для регистрации</i>	67
<i>Параметры дозвона — Dialing</i>	67
<i>Параметры дозвона — Callback</i>	68
<i>Параметры дозвона — Appearance</i>	69
<i>Параметры дозвона — Phone book</i>	71
Автоматическая регистрация в системе	72
Элементы управления персональным доступом	73
<i>Определение персонального доступа к файлу с помощью File Manager</i>	74
<i>Определение персонального доступа к принтеру с помощью Print Manager</i>	74
<i>Определение персонального доступа для учетной записи пользователя с помощью User Manager for Domains</i>	75
Маркеры доступа	76
Списки контроля доступа	76
 IV Администрирование учетных записей пользователей	 79
Учетные записи пользователей	80
Локальные и глобальные учетные записи	80
Сквозная авторизация	83
Создание и редактирование учетных записей пользователей	84

Пароль пользователя и правила его модификации	85
Создание учетных записей пользователей с помощью программы-мастера	87
Группы пользователей	88
Локальные группы	89
Локальные группы на рабочих станциях	91
Локальные группы домена	91
Встроенные локальные группы	91
Глобальные группы	92
Глобальные группы, встроенные в Windows NT Server	93
Стратегия использования групп	94
Создание и модификация групп	95
Создание локальной группы	95
Создание глобальной группы	97
Модификация локальной группы	98
Модификация глобальной группы	98
Создание и модификация групп с помощью программы-мастера Group management Wizard	99
Специальные группы	99
Группа Network	100
Группа Interactive	100
Группа Everyone	100
Группа Creator Owner	101
Права и привилегии пользователей и групп	101
Привилегии встроенных учетных записей	104
Учетная запись Guest	104
Учетная запись Administrator	105
Привилегии встроенных локальных групп	106
Привилегии группы Users	106
Привилегии группы Power Users	107
Привилегии группы Administrators	108
Привилегии группы Guests	109
Привилегии группы Backup Operators	109
Привилегии группы Server Operators	109
Привилегии группы Account Operators	110
Привилегии группы Print Operators	110
Изменение привилегий пользователей	111
Включение пользователей в группы	112
Изменение определенных привилегий пользователя	112

Профили пользователей	113
Обязательные и персональные профили	115
Создание и редактирование профилей	116
Сохранение профиля	118
Домашние каталоги — персональные хранилища	120
Сценарии регистрации (Logon Scripts)	122
Ограничение времени работы пользователей	123
Ограничение числа рабочих станций, с которых возможна регистрация	124
Использование Редактора системной политики в Windows NT Server 4.0	125
Системная политика по отношению к пользователям	126
Системная политика по отношению к компьютерам	126
Два режима работы Редактора системной политики	127
Два вида загрузки системной политики	130
Групповая политика	131
Параметры системной политики	133
Шаблоны для формирования системной политики	142
Определение общих параметров учетной записи	143
Управление политикой ведения учетных записей	144
Установка максимального срока действия пароля	145
Изменение минимальной длины пароля	146
Установка продолжительности запрета на изменение пароля пользователем ...	146
Хранение истории паролей	147
Блокировка учетных записей	147
Принудительное отключение удаленных пользователей по истечении разрешенного времени работы	148
Обязательность регистрации для смены пароля	148
Блокировка рабочей станции	148
 V Файловая система NTFS	 151
Файловые системы Windows NT	152
Файловая система FAT	153
Файловая система HPFS	154
Файловая система NTFS	156
Главная файловая таблица	156
Целостность данных и восстановление в NTFS	157
Длинные и короткие имена файлов	158

Компрессия файлов и каталогов	160
Создание и модификация разделов диска	162
Преобразование существующего раздела в формат NTFS	164
Права на доступ к файлам и каталогам. Понятие владельца	165
Предоставление прав на доступ к файлам	166
Предоставление прав на доступ к каталогам	169
Владение каталогами и файлами	173
Стратегия предоставления прав на доступ	174
Использование прав на доступ на разделах FAT и HPFS	175
File Delete child	175
Совместное использование в сети	176
Защита предоставляемых для совместного использования каталогов на томах FAT или HPFS	176
Защита предоставляемых для совместного использования каталогов на томах NTFS	177
Предоставление файлов и каталогов в совместное использование	178
Повторное предоставление ресурсов в совместное использование	181
Просмотр предоставленных ресурсов и отмена совместного использования	182
Тиражирование каталогов	183
Конфигурирование компьютеров экспорта и импорта	185
Защита тиражирования	186
 VI Обеспечение отказоустойчивости	 189
Средства повышения надежности работы с диском	190
Проверка состояния жесткого диска	190
Технология RAID (Избыточный массив недорогих дисков)	192
Чередование дисков	192
Зеркализация и дублирование дисков	193
Чередование дисков с записью кода коррекции	194
Чередование дисков с записью кода коррекции в виде четности	194
Чередование дисков большими блоками. Хранение четности на одном диске ..	194
Чередование дисков с записью информации о четности на все диски	194
Замена секторов в "горячем режиме"	195
Резервное копирование на магнитную ленту	195

Встроенная поддержка	196
<i>Продукты сторонних фирм</i>	<i>197</i>
Arcada Backup Exec	197
Cheyenne ARCserve®	198
Palindrome Backup Director Windows NT Edition v.4.0.....	199
Обеспечение бесперебойного питания	199
Встроенная поддержка UPS	199
Продукты сторонних фирм	200
Выбор работоспособной конфигурации	200
Выбор профиля техники	201
Emergency Repair Disk	202
Зеркализация серверов	203
Кластеры серверов	205
Определение кластеров	205
<i>Иллюстрация кластеров — доступность данных</i>	<i>206</i>
<i>Иллюстрация кластеров — наращиваемость</i>	<i>207</i>
Традиционная архитектура предоставления высокой доступности	207
Традиционная архитектура обеспечения наращиваемости	208
Архитектура кластера	208
<i>Модель с общими дисками</i>	<i>208</i>
<i>Модель без общих компонентов</i>	<i>209</i>
Серверы кластерных приложений	210
Кластеры на основе Windows NT Server	210
<i>Двухфазный подход</i>	<i>210</i>
 VII Разграничение доступа к принтерам	 213
Работа с принтерами	214
Создание принтера	214
Совместное использование принтеров	216
Настройки принтера	217
Права доступа к принтеру	220
Владелец	221
Защита спул-файла	222
Защита реестра	222

VIII	Взаимодействие с Novell Netware	223
	Основные виды взаимодействия	224
	Доступ к серверным приложениям Windows NT Server	225
	Доступ с Windows NT Server и Windows NT Workstation к серверам Netware	226
	Обеспечение прозрачного доступа клиентов сети Microsoft	
	к ресурсам сети Novell	228
	Обеспечение прозрачного доступа клиентов сети Netware	
	к файлам и принтерам доменов Windows NT Server	229
	Централизованное управление серверами Netware	233
	Переход от сервера Netware к Windows NT Server	236
IX	Построение глобальных сетей и работа с Internet	241
	Удаленный доступ в Windows NT	242
	Маршрутизация в Windows NT	243
	Многопротокольная маршрутизация в Windows NT Server	244
	Возможности маршрутизации	244
	Установка маршрутизации между локальными сетями	245
	Статическая маршрутизация по IP	246
	Маршрутизация через коммутируемый канал связи	247
	Параметры организации маршрутизации	248
	Повышение пропускной способности канала	250
	Сети X.25	252
	Point-to-Point Tunelling Protocol (PPTP)	254
	Обеспечение безопасности при удаленном доступе	256
	Доменная основа защиты	256
	Централизованные домены	257
	Распределенные домены	257
	Привилегия удаленного доступа	257
	Аутентификация удаленного доступа	259
	Обратная связь	260
	Поддержка защитных хостов	261
	Отключение пользователей	261
	Ограниченный доступ к сети	262
	Предоставление доступа только к серверу	262
	Предоставление доступа только к части сети	263

Шифрование данных	263
Конфигурирование клиентской части в Windows NT 4.0	264
<i>Выбор альтернативного номера</i>	265
<i>Возобновление связи</i>	266
<i>Доступность информации</i> <i>об удаленном доступе</i>	268
Безопасная работа с Internet	269
Предоставление одностороннего доступа в Internet	270
Часть локальной сети как ресурс Internet	271
 X Использование реестра	 275
Назначение реестра	276
Структура реестра	276
Ульи и файлы	279
Целостность и восстановление улья в реестре	279
Ограничение доступа к реестру	280
Использование реестра для быстрого восстановления конфигурации 32-разрядных приложений	282
 XI Аудит и мониторинг системы	 283
Аудит в Windows NT	284
Аудит системных событий	285
Аудит доступа к файлам и каталогам	287
Аудит реестра	288
Аудит печати	290
Аудит сервера удаленного доступа	291
Аудит Книги обмена	293
Журналы регистрации событий защиты	294
Сигналы тревоги (Alerts)	298
Анализ и настройка производительности сервера с помощью программы Performance Monitor	301
Поиск и терминирование отдельных процессов	304
Анализ загруженности системы в Windows NT 4.0	307

XII Приложения	309
Установки, обеспечивающие минимальную защиту	310
Требования физической защиты	310
Требования программной защиты	310
Установки, обеспечивающие обычную защиту	311
Требования физической защиты	311
Требования программной защиты	311
Предупреждение при регистрации	311
Учетные записи пользователей и группы	312
Защита файлов и каталогов	312
Защита реестра	313
Аудит	313
Управление журналом безопасности	314
Установки, обеспечивающие высокую степень защиты	315
Требования физической защиты	315
Сети и безопасность	315
Контроль за доступом к выключателю питания	315
Требования программной защиты	316
Привилегии пользователей	316
Защита файлов и каталогов	319
Защита реестра	320
Сервис планирования (команда AT)	321
Скрытие имени последнего пользователя	321
Ограничение процесса загрузки	322
Разрешение выключать компьютер	
только зарегистрированным пользователям	322
Контроль за доступом к съемным устройствам хранения	323
Установки, необходимые для соответствия защиты уровню C2	325
Системы, на которых Windows NT	
сертифицирован на соответствие уровню C2	334
Compaq ProLiant 2000 и 4000	334
Проверка целостности процессора	335
Проверка целостности периферии	335
DECpc AXP/150	335
Проверка целостности процессора	336
Проверка целостности периферии	336
Словарь терминов	337
Предметный указатель	363

Основные свойства Windows NT

Операционные системы Microsoft Windows NT и Windows NT Advanced Server появились в продаже в июле 1993 года. Тогда их использовали лишь энтузиасты и крупные компании. Во многом это было связано с довольно высокими требованиями системы к аппаратуре. С выходом версии 3.5, заметно снизившей уровень этих требований и включившей в себя ряд новых функций, начался стремительный рост популярности Windows NT. Сегодня она широко применяется самыми разными организациями, банками, промышленностью и индивидуальными пользователями. Все больше становится поклонников этой удобной и надежной системы и в России. Версия 4.0 — это следующий шаг в распространении Windows NT: новый интерфейс и масса новых полезных свойств привели к широкому внедрению этой системы на персональных рабочих местах.

Приоритетная многозадачность

Ранние версии Windows поддерживали неприоритетную многозадачность, из-за чего работа системы зависела от корректности запущенных задач. Все приложения делили процессорное время путем периодического опроса друг друга. Если какое-либо приложение отказывалось отвечать, система не знала, что в таком случае делать. В Windows NT действует принцип приоритетов, позволяющий приложениям с более высоким приоритетом “вытеснять” имеющие более низкий. Так как система всегда контролирует события, процессорное время используется эффективнее, а “сбойное” приложение не приведет к зависанию системы.

Встроенная сетевая поддержка

В отличие от большинства других операционных систем для персональных компьютеров Windows NT изначально создавалась с учетом работы в сети. Поэтому функции совместного использования файлов, устройств и объектов встроены в интерфейс пользователя. Администраторы могут централизованно управлять и контролировать работу сетей в масштабах крупных предприятий. Особенно важна возможность распространения работы приложений типа клиент-сервер на многокомпьютерные системы.

Защищенность

Система Windows NT сертифицирована в США на уровень защиты C2 по Оранжевой книге, что подразумевает возможность владельца ресурсов (файла, каталога, принтера или совместно используемого объекта данных) управлять доступом к ним. C2 гарантирует изолированное выполнение приложений в системе и обязывает пользователей регистрироваться. При этом можно указать разные уровни доступа к ресурсам, предоставляя определенным пользователям или группам один из таких уровней, а операционная система определит, был ли доступ к ресурсу удачным.

Многопоточность

Поддерживаемая в Windows NT многопоточность позволяет определенным образом разработанным приложениям одновременно выполнять несколько собственных процессов. Так, работая с многопоточной электронной таблицей, пользователь может выполнять перерасчет в одной таблице, в то время как печатается другая и загружается в память третья. Наглядно многопоточность проявляется в графических приложениях, позволяя запустить сложную обработку одного образа и сразу перейти к редактированию другого или печати третьего.

Поддержка симметричной мультипроцессорной обработки

Windows NT поддерживает работу на компьютерах с несколькими процессорами. Эти системы становятся все популярнее, по мере того как приложения для мини-ЭВМ и мэйнфреймов переносятся на платформу ПК. Назначая различные потоки для разных процессоров, Windows NT повышает производительность приложений, требующих большой вычислительной мощности.

Бытует мнение, что сервер Windows NT не работает в системах с числом процессоров, превышающим 4. Это не так. Система способна поддерживать до 32 процессоров. Из чисто практических соображений стандартная версия имеет ограничение на 4 поддерживаемых процессора. Но ведь именно 4 процессора — предел и для абсолютного большинства моделей: полистайте рекламные буклеты компаний, выпускающих компьютеры! Если у Вашего компьютера много процессоров, Вы получите от фирмы-производителя такой техники необходимый модуль поддержки, но уже за дополнительную плату.

Поддержка широкого спектра компьютерных платформ

Windows NT можно установить на самых различных типах компьютеров, список которых продолжает расти. Сегодня поддерживаются Intel-компьютеры с процессорами 386, 486, Pentium и Pentium Pro, а также три типа RISC-процессоров: PowerPC, MIPS R4000 и DEC Alpha. Благодаря особенностям внутренней структуры, Windows NT на другие платформы перенести довольно просто.

Возможность выполнения приложений, написанных для других операционных систем

Операционная система, не позволяющая выполнять уже существующие приложения, обречена. В Windows NT работают практически все 16-разрядные приложения для Windows, MS-DOS, неграфические 16-разрядные приложения для OS/2 и POSIX-приложения. Дополнительные подсистемы позволяют работать 16-разрядным PM-приложениям и UNIX-приложениям, соответствующим стандарту POSIX.2.

Поддержка нескольких файловых систем

Кроме возможности выполнения приложений, написанных для других операционных систем, в Windows NT поддерживаются и различные типы файловых систем. Можно использовать жесткий диск, отформатированный в одной из трех систем: FAT, HPFS и NTFS, разработанной специально для Windows NT. Очень надежная, NTFS позволяет применять длинные имена файлов и контролировать доступ к определенным файлам. В 4 версии файловая система HPFS больше не поддерживается, так как не предлагает никаких преимуществ по сравнению с двумя другими и гораздо меньше распространена.

Знакомый интерфейс

Если Вы один из миллионов пользователей Microsoft Windows, то, несомненно, заметите, что интерфейс Windows NT практически не отличается от привычного. Версии Windows NT до 3.51 включительно имели интерфейс Windows 3.x. В новой, четвертой версии используется интерфейс, идентичный принятому в Windows 95 с незначительными отличиями, связанными с особенностями Windows NT.

Интеллектуальная программа установки

Если Вы умеете устанавливать Windows для рабочих групп или Windows 95, то с Windows NT проблем у Вас не будет: ведь программа установки сама распознает сетевые платы компьютера и их параметры, протоколы, используемые в сети, позволит быстро установить и проверить видеорежимы и многое другое. Добавленная в версии 4.0 возможность "отчужденной" установки, при которой не требуется вмешательство пользователя, позволяет легко и быстро установить операционную систему на большое количество компьютеров предприятия.

Различие между версиями Windows NT

Windows NT выпускается в двух версиях: рабочая станция *Windows NT Workstation* и сервер *Windows NT Server*. Хотя Windows NT Workstation может выполнять функции невыделенного сервера в одноранговой сети, использовать ее вместо полноценного сервера нельзя. Связано это с отсутствием в ней средств администрирования и управления доменом, оптимизации подсистем для исполнения только приложений и введенным ограничением на число одновременных подключений.

Функции Windows NT Server

Windows NT Server может выступать как:

- файл-сервер;
- сервер печати;
- сервер приложений;
- контроллер домена;
- сервер удаленного доступа;
- сервер Internet;
- сервер обеспечения безопасности данных;
- сервер резервирования данных;
- сервер связи;
- сервер вспомогательных служб.

Windows NT Server как файл-сервер

Эта функция вполне ясна: компьютер используется как централизованное хранилище файлов, коллективно используемых в офисе или хранение которых на локальном компьютере нецелесообразно. Для организации файл-сервера не надо специальной подготовки вроде монтирования томов. Все файловые ресурсы независимо от того, на каком диске они расположены (жестком или CD-ROM), сразу могут быть предоставлены для совместного доступа.

Windows NT Server как сервер печати

Windows NT Server позволяет работать и предоставлять в совместное пользование неограниченное число принтеров. Они могут быть подключены локально или по сети с помощью протоколов TCP/IP и DLC.

В качестве рабочих станций могут выступать компьютеры с MS-DOS, Windows для рабочих групп, OS/2, Macintosh, Windows NT Workstation. Если Вы хотите с рабочей станции в системе Windows NT Workstation подключиться к удаленному принтеру, предоставляемому Windows NT Server, просто выберите этот принтер из числа доступных. Система не будет просить у Вас дискеты с драйверами и т.п. — просто использует драйвер, установленный на сервере!

Windows NT Server как сервер приложений

В последнее время растет нужда в системах, способных исполнять основное — “тяжелое” — приложение на мощном высокопроизводительном сервере, а результаты деятельности по запросам передавать на маломощные клиентские станции, реализуя модель клиент-сервер. Переход с больших мейнфреймов на современные системы на базе ПК средней и большой мощности как раз и требует такого решения.

Изначально построенная по схеме клиент-сервер, Windows NT отлично приспособлена для работы в системах клиент-сервер в качестве сервера приложений. В первую очередь такими приложениями являются системы управления базами данных, системы информационного обмена, системы управления. Именно поэтому в Microsoft BackOffice входят Microsoft SQL Server — сервер баз данных, Microsoft System Management Server — сервер управления системой, Microsoft Exchange — сервер информационного обмена, SNA Server — сервер связи с мейнфреймами и Internet Information Server — сервер Internet.

Кроме приложений корпорации Microsoft, существует более 2000 разработок других фирм: серверы баз данных (Informix, Oracle, IBM и т.д.), системы управления сетями (HP, DEC), управления производством (SAP), документооборота (Lotus, Saros), финансовые (Platinum) и многие другие системы для бизнеса.

Windows NT Server как сервер резервирования данных

В Windows NT встроена возможность резервного копирования файлов на магнитную ленту. Администратор системы определяет пользователя, ответственного за эту операцию, и регулярно выполняет копирование данных на стример только он. Эту операцию можно автоматизировать.

Windows NT Server как сервер удаленного доступа

Служба удаленного доступа (Remote Access Service — RAS) состоит из двух частей: серверной — устанавливаемой на компьютере с Windows NT Server, и клиентской — устанавливаемой на компьютерах с MS-DOS, Windows for Workgroups, Windows 95 или Windows NT Workstation.

Пользователь рабочей станции, связанной с сетью через сервер удаленного доступа, чувствует себя работающим непосредственно в сети: он может осуществлять доступ к файлам и данным, печатать документы, подключаться к хостам через SNA Server и обмениваться с коллегами сообщениями по электронной почте.

Такой прозрачный доступ к сети удобен тем, кто постоянно бывает в разъездах, командировках, и администраторам системы. RAS широко применяется и для связи территориально удаленных филиалов предприятий. Одновременно через протоколы PPP и SLIP поддерживается до 256 сессий удаленного доступа.

Набор протоколов Point-to-Point Protocol (PPP) позволяет осуществлять удаленный доступ в условиях разнородной сети. Поддержка PPP гарантирует возможность удаленного доступа через любой стандартный PPP-сервер удаленного доступа. С другой стороны, Windows NT Server способен соединяться и обеспечивать доступ к сети для пользователей, применяющих средства удаленного доступа сторонних производителей, таких как Netware Connect, Shiva Lanover и др.

RAS в Windows NT Server поддерживает любую комбинацию протоколов TCP/IP, IPX/SPX и NetBEUI при удаленном доступе. Поддержка IPX делает NT Server идеальным сервером удаленного доступа для сетей NetWare.

Поддержка протокола TCP/IP выводит NT Server в разряд систем, готовых к работе в Internet. Вы можете подключаться к Internet через его сервер удаленного доступа и просматривать ресурсы Internet, используя его средства поиска и просмотра.

Windows NT Server как сервер связи сетей

Говоря о Windows NT Server как о сервере связи, подразумевают возможность соединения различных сегментов сети.

Замечательное свойство Windows NT Server — возможность сопряжения разнородных сетей. Если Вы уже имеете сеть Novell Netware, соединение ее с Вашим новым офисом не составит труда. Популярность Windows NT неуклонно растет, и ряд фирм выпустил продукты, обеспечивающие совместную работу с другими сетями. Редиректор фирмы Banyan позволяет Windows NT функционировать в качестве клиента в сети Banyan VINES®. Для прозрачного подключения к сетям UNIX имеются продукты, обеспечивающие клиентскую и серверную части NFS (Network File System). Кроме TCP/IP и NFS, другим общим сетевым стандартом для UNIX является X-Window. В настоящее время несколько фирм, в том числе DEC, AGE Logic, Hummingbird, Intergraph и Visionware выпустили X-серверы.

Главная проблема администрирования

Обширный набор функций и свойств, естественно, вызвал к Windows NT повышенный интерес. Тысячи администраторов сетей, разработчиков программно-го обеспечения и просто пользователей устанавливают эту систему на компьютеры, включают в состав существующих систем или создают новые сети, использующие только технологии Microsoft... Но здесь-то и подстерегает основная трудность — отсутствие у администраторов знаний и опыта работы с сетями Microsoft. Пришедшие в основном из мира NetWare, они пытались перенести на NT Server идеологию и способы администрирования этой сетевой ОС. Недопонимание роли доменной организации сетей приводило к тому, что как “гуру от Netware”, так и новички не могли обеспечить централизованного управления сетью, грамотно распорядиться сетевыми ресурсами, распределить права и привилегии пользователей, что в целом сказалось на надежности и защищенности таких систем.

Думается, проблема вызвана нехваткой информации. Вопрос информационной поддержки пользователей Windows NT особенно остро стоит в России. К сожалению, зарубежные издания либо не доходят до нас, либо просто не по карману администратору сети госпредприятия. Надеемся, эта книга в какой-то степени разрядит ситуацию и ответит на большинство вопросов пользователей, начинающих работать в Windows NT.

Об этой книге

Книга *Windows NT Server: администрирование и надежность*, вышедшая в апреле 1996 года, была раскуплена практически сразу. С одной стороны, это подтверждение высокого интереса к Windows NT, с другой — свидетельство катастрофической нехватки литературы на эту тему. Поэтому была начата подготовка второго издания книги. Однако в процессе работы, в которой существенно помогли поступившие к тому времени отклики читателей и прессы, постепенно становилось ясным, что переиздание превращается в новую книгу. Поэтому, несмотря на совпадение некоторых разделов с соответствующими разделами в *Windows NT Server: администрирование и надежность*, читатель не может не заметить, что держит в руках фактически другую книгу. Добавлены главы о планировании и установке операционной системы, о взаимодействии с Novell Netware, Вы найдете большое количество практических советов, касающихся поддержки русского языка, работы с файлами и каталогами. Значительно шире представлены проблемы построения кластеров на базе Windows NT Server и способы организации глобальных сетей. Особое внимание уделено новой версии Windows NT 4.0.

Наивно полагать, что одна книга заменит несколько томов документации, поставляемой с Windows NT Server. Не рассчитывайте найти здесь синтаксис команд, расшифровку сообщений об ошибках системы или объяснение внутреннего устройства отдельных драйверов и подсистем. Информация такого рода содержится в специализированном пятитомном издании Windows NT Resource Kit, выпускаемом Microsoft Press (в настоящее время два тома изданы на русском языке).

Книга *Windows NT — выбор "профи"* обобщает опыт практической работы с системами на базе Windows NT. Здесь освещены проблемы, с которыми сталкивается практически каждый. Материал подан в такой последовательности, что новички, делающие первые шаги в сетях, читая книгу с самого начала, быстро поймут идеологию сетей на базе Windows NT и смогут самостоятельно спланировать и сконфигурировать свою систему. Пользователи из мира других сетевых ОС могут пропустить главы с описанием хорошо знакомых для них понятий. Тем, кто уже какое-то время работает с системами на базе NT Server, книга понадобится как краткий справочник с рекомендациями по планированию и выбору техники, использованию доменов, учетных записей пользователей и групп, осуществлению доступа к Internet. Столкнувшись с неясным термином, поищите разъяснения в словаре в конце книги.

Проблему надежной работы сетевой ОС можно разделить на две большие части: обеспечение бесперебойной работы системы и обеспечение защиты данных, хранящихся в этой системе. И то и другое достигается за счет умелого администрирования, которое невозможно без понимания *доменов Windows NT* и *взаим-*

моотношений между ними, а также без четкого представления об устройстве системы безопасности. Эти разделы и вынесены в начало книги.

Как показывает опыт общения с пользователями, знание теоретических основ построения сети не всегда помогает в реальной жизни. Правильно выбрать тип и конфигурацию компьютеров, сетевых протоколов и не сделать типичных ошибок при установке системы поможет глава *Планирование и установка*.

Понятия *учетных записей* пользователей и *групп* — это краеугольный камень в разграничении доступа к ресурсам системы. Знание стратегии их применения и разумная политика ведения учетных записей обеспечат Вашу уверенность в надежной защите информации от посторонних глаз. Эти вопросы освещены в главе *Администрирование учетных записей пользователей*.

Файловая система Windows NT — NTFS — для многих все еще terra incognita. Понять, почему NTFS обеспечивает высокую степень отказоустойчивости Windows NT, как использовать дисковые массивы, и узнать о средствах резервного копирования и обеспечения бесперебойного питания Вы сможете из глав *Файловая система NTFS* и *Обеспечение повышенной отказоустойчивости при работе с файлами и каталогами*.

В какой организации нет принтера! Печатать надо всегда и всем: служебные записки и диссертации, отчеты и стихи, любовные послания и кляузы, — в общем все, что терпит бумага, а терпит она все. Как сделать так, чтобы Ваш личный документ не попал в чужие руки, рассказывается в главе *Разграничение доступа к принтерам*.

Вы до этого работали исключительно с Netware? Вы продолжаете использовать эту систему, но хотите "запрячь" ее в одну упряжку с Windows NT? Пожалуйста! Обо всех возможностях совместной работы этих систем читайте главу *Взаимодействие с Netware*.

Одна из самых горячих тем на сегодняшний день — объединение нескольких локальных сетей в глобальную и безопасное подключение к Internet. Вы найдете в книге рекомендации по использованию протокола TCP/IP, настройке *сервера удаленного доступа*, обеспечивающей надежную защиту Вашей сети от внешнего вторжения; маршрутизации в глобальных сетях. Все это читайте в главе *Построение глобальных сетей и работа с Internet*.

Если Ваша система работает исправно, но Вы продолжаете терзаться сомнениями о честности отдельных пользователей или опасаетесь вторжения нового коварного вируса, способного уничтожить не только данные, но и всю систему, значит, займитесь *аудитом*. Оптимальной организации аудита посвящена отдельная глава.

Ну и наконец, Вам известно, что Windows NT обеспечивает защиту данных в соответствии с уровнем C2. А нужна ли Вам такая защита? Может, хватит менее суровых мер? Или Вы не уверены, что Ваша система соответствует C2? Тогда воспользуйтесь практическими рекомендациями по настройке различных степеней защиты — они приведены в *Приложениях*. Можете смело доверять этой информации — официальным рекомендациям фирмы Microsoft.

Разделы книги, посвященные Windows NT версии 4.0, отмечены специальным значком и особо оформлены.

Служба каталогов Windows NT

Эффективность управления большими сетями во многом определяется их структурой, или, как еще говорят, — службой каталогов. В сетях, построенных на основе Windows NT Server, применяется так называемая служба каталогов NTDS (Windows NT Directory Service), основанная на взаимодействии доменов. Использувавшаяся ранее в сетях на основе Microsoft LAN Manager, она долго не находила широкого применения из-за неудобства работы с ней в крупных сетях. Для Windows NT Server она была существенно переработана: например, реализована возможность установления между доменами доверительных отношений, что позволяет формировать структуру сети в полном соответствии со структурой предприятия.



Сетевые модели: рабочие группы и домены

В сетях на основе Windows NT используются две модели построения сети: *модель рабочих групп* (workgroup model) и *модель доменов* (domain model). В этом разделе мы рассмотрим их различия и поговорим о *доверительных отношениях* (trust relationships) между доменами, позволяющих упростить управление большой сетью со множеством доменов.

Модель рабочих групп

Рабочая группа (workgroup) — это организационная единица, представляющая собой набор сгруппированных вместе компьютеров. Рабочие группы позволяют объединять рабочие станции, не входящие в домен (domain). У каждого компьютера с Windows NT имеется своя база учетных записей и своя политика защиты.

Администрирование рабочей группы аналогично администрированию одного компьютера. Все выполняемые административные действия применяются только к одной рабочей станции.

Зачем же такая организация нужна, что она дает? Ответ прост. С позиции пользователя, это простой способ визуального группирования компьютеров при просмотре доступных сетевых ресурсов. Пользователю легче осуществлять доступ к компьютерам в своей группе — на экране они собраны в одном месте. При этом независимо от того, сколько реально компьютеров в отделе или подразделении, пользователь имеет дело только с этой группой и не тратит время на поиски нужного.

Отдельно стоящая рабочая станция на основе Windows NT — частный случай рабочей группы, состоящей из одного компьютера. При этом может даже не быть постоянных связей данной рабочей станции с другими компьютерами. Это не самый популярный способ работы в Windows NT, но иногда возникает необходимость в индивидуальной защите каждой рабочей станции. В отличие от других операционных систем (вроде MS-DOS или OS/2) отдельно стоящий компьютер Windows NT обладает встроенной процедурой регистрации и контроля доступа.

Доменная модель

По мере роста управление рабочей группой усложняется в силу полной децентрализации баз учетных записей и средств защиты. Для обеспечения надежной защиты и упрощения управления сетью Windows NT Server предлагает *доменную модель*.

Доменом называется совокупность компьютеров, характеризующаяся наличием *общей базы учетных записей пользователей и единой политики защиты*. Централизованные средства управления учетными записями пользователей и *политикой защиты* позволяют администратору эффективно поддерживать защиту системы в рамках отдела, подразделения и всего предприятия.

У каждого домена есть свое уникальное имя, которое отражает либо его функциональное назначение (скажем, DEVELOPERS_DOM), либо местонахождение (MOSCOW_EAST), либо что-то, понятное Вам одному (вроде MASTER_DOM1). Помните: русские символы в имени домена использовать нельзя, так как это может вызвать проблемы совместимости.



Замечание: Возможно, Вы знакомы с понятием доменов в UNIX-сетях. Так вот: домены Windows NT ничего общего с ними не имеют.

Администрирование домена

В Windows NT Server администрирование переносится с одного компьютера на весь домен. Независимо от числа компьютеров в домене администратор имеет дело только с одной учетной записью для каждого пользователя, а у каждого пользователя есть только одна учетная запись. Компьютер в домене, на котором хранится база учетных записей всего домена, называется *первичным* (или *главным*) *контроллером домена* (Primary Domain Controller — PDC). Для обеспечения надежного хранения столь важной информации Windows NT Server тиражирует ее на другие компьютеры домена — *резервные контроллеры домена* (Backup Domain Controller — BDC). Это гарантирует сохранность важной информации при выключении или сбое первичного контроллера домена. Такая структура позволяет также минимизировать средства аппаратной защиты, оснащая ими только контроллеры домена, и ограничить доступ к этим, наиболее критичным, компонентам сети, установив их в отдельном помещении, лучше всего — физически защищенном.

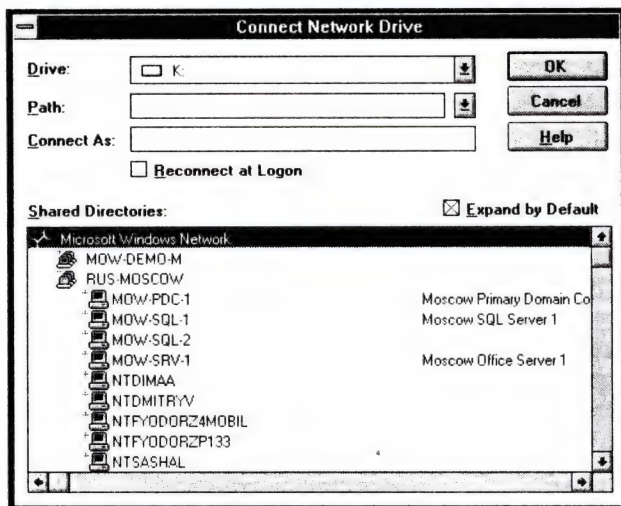
Кроме контроллеров домена (PDC и BDC), в состав домена могут входить *серверы* (servers) — компьютеры, работающие под управлением Windows NT, но не выполняющие функции контроллера домена: файл-серверы, серверы печати или приложений. На них, например, могут выполняться приложения, входящие в Microsoft BackOffice.

Серверы включаются в домен, если:

- на сервере должны выполняться критичные по надежности и быстродействию приложения и он не должен тратить времени на регистрацию пользователей и тиражирование базы Security Account Manager (SAM) на другие серверы;
- администратору этого сервера нельзя быть администратором всего домена;

- в будущем планируется перенести сервер в другой домен;
- сервер нужно использовать для администрирования серверов домена.

При просмотре сетевых ресурсов пользователь видит все компьютеры, включенные в домен, в виде групп, названных аналогично представляемым на экране рабочим группам.



Отображение на экране доменов и входящих в них компьютеров.

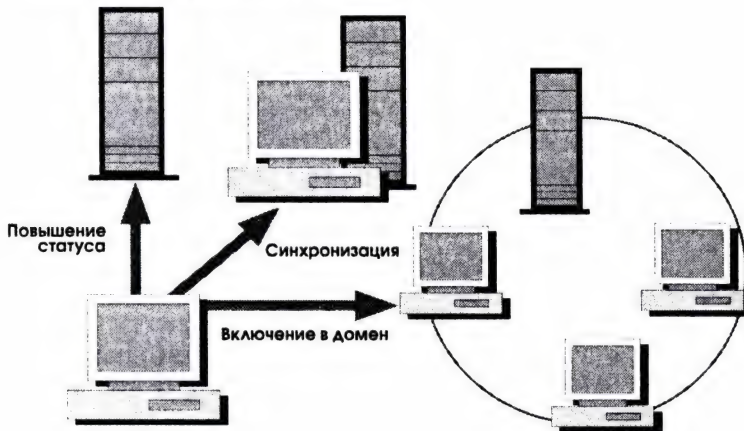
В каждом домене может быть только один первичный контроллер домена. Все изменения, вносимые в базу учетных записей пользователей SAM (см. главу *Система безопасности Windows NT*), выполняются только на этой машине. Компьютер, выполняющий роль первичного контроллера домена, можно изменить с помощью **Server Manager**, входящего в поставку Windows NT Server. Для этого в **Server Manager** выберите имя сервера, который должен стать первичным контроллером домена. Он обязательно должен быть резервным контроллером. После этого выберите команду **Promote to Primary**.

В течение некоторого времени после исполнения этой команды будет идти синхронизация баз SAM. Повышение статуса BDC до статуса PDC автоматически понижает статус прежнего PDC до уровня BDC.

А надо ли вообще менять статус контроллера? Рассмотрим простой пример. Допустим, Вы администратор крупной сети с десятками пользователей и соби-

раетесь поменять компьютер, выполняющий роль первичного контроллера домена. Если просто установить Windows NT Server на новый компьютер и объявить его первичным контроллером домена, то, во-первых, имя этого домена будет иным (так как имена доменов в сети уникальны), а во-вторых, на нем придется заново создавать учетные записи всех пользователей, переопределяя права доступа к ресурсам на всех остальных серверах. Чувствуете, во что это выльется? Если же объявить новый сервер резервным контроллером существующего домена, то после повышения его статуса до PDC (это дело нескольких минут) можно выключить бывший первичный контроллер без малейшего ущерба для работы сети (конечно, если этот сервер не выполнял больше никаких других функций).

Администрирование домена



Резервные контроллеры домена — BDC — обеспечивают доступ к базе SAM только в режиме чтения. BDC (в домене их может быть несколько) может отвечать на запросы об учетных записях и идентифицировать пользователя, но не вносить изменения в базу SAM.

Пользователи, не являющиеся членами домена, по определению не имеют прав доступа к ресурсам домена. Как говорится, “мой ДОМен — моя крепость”. Пользователь в домене как за каменной стеной: ни к нему никто не ворвется снаружи, ни он не сделает ни шагу за границы домена.

На предприятии домены можно организовать по самым разным признакам: функциональному, территориальному и др. Подробнее о способах организации доменов я расскажу ниже.

Нагрузочная способность доменов

В каждом домене содержатся учетные записи пользователей, машин и групп как встроенных, так и созданных (см. раздел *Группы пользователей*). Каждый из этих объектов занимает место в базе SAM. Практическое ограничение на размер файла базы SAM зависит от типа процессора и от объема оперативной памяти компьютера, используемого для администрирования домена. Предвижу недоуменные и даже схишные возгласы: а разве объем базы SAM зависит от типа процессора? Дело в том, что одним из критериев определения этого объема является время загрузки файла базы при администрировании, а также время аутентификации пользователя. Понятно, что чем больше размер базы и чем больше в ней хранится учетных записей, тем дольше идет регистрация. Естественно, чем производительней процессор, тем быстрее выполняется авторизация пользователей. Microsoft рекомендует максимальный размер файла базы SAM в 40 Мб. Файлы большего размера требуют значительного времени загрузки при администрировании.

Различные типы объектов занимают в базе разное пространство:

Объект	Используемый объем
учетная запись пользователя	1,0 Кб
учетная запись машины	0,5 Кб
учетная запись группы	4,0 Кб

Ниже приведены примеры распределения объектов в базе SAM:

	Учетные записи пользователей	Учетные записи машин	Учетные записи групп	Общий объем базы SAM
1 рабочая станция на 1 пользователя	2 000	2 000	30	3,12 Мб
2 рабочих станции на 1 пользователя	5 000	10 000	100	10,4 Мб
2 пользователя на 1 рабочую станцию	10 000	5 000	150	13,1 Мб
1 рабочая станция на 1 пользователя	25 000	25 000	200	38,3 Мб
1 рабочая станция на 1 пользователя	26 000	26 000	250	40 Мб
1 рабочая станция на 1 пользователя	40 000	0	0	40 Мб

Как видите, в одном домене может быть до 40 000 учетных записей пользователей. Используя модели нескольких мастер-доменов (см. ниже), сеть может включать до 100 000 учетных записей пользователей.

Доверительные отношения

В доменной модели защита реализуется с помощью Windows NT Server установлением *доверительных отношений*. Так называется связь между доменами, позволяющая пользователям одного домена узнать о пользователях и ресурсах другого. В доверительных отношениях участвуют доверяющий домен (trusting domain) и доверяемый домен (trusted domain). Доверяющий домен распознает учетные записи всех пользователей и групп пользователей доверяемого домена. Эти учетные записи можно поместить в локальные группы доверяющего домена для назначения им прав и привилегий. (Подробнее о группах, правах и привилегиях см. раздел *Группы пользователей*.) Доверительные отношения позволяют пользователю, имеющему учетную запись в одном домене, осуществлять доступ к ресурсам всей сети.

Доверительные отношения — это, по сути, административные и коммуникационные связи. Когда они установлены, пользователи одного домена могут обращаться к ресурсам другого. И все же в большей степени такие отношения — средство администрирования, а не параметр, присваиваемый системой пользователю, и их надо рассматривать с точки зрения администрирования учетных записей, но не как возможность использования ресурсов.

Доверительные отношения упрощают администрирование сети путем объединения двух и более доменов в один административный узел. Допустим, при наличии четырех доменов стандартная схема предполагает четыре различные базы SAM с раздельным администрированием. Установив же между доменами доверие, Вы обойдетесь одной базой и небольшим количеством групп.

Подчеркнем: первое преимущество доверительных отношений в том, что пользователь получает доступ ко всем ресурсам сети, не выполняя дополнительной регистрации. И второе: администратор сети может управлять всей сетью с одного места. Для установления доверительных отношений необходимо, чтобы в состав сети входил Windows NT Server.

Типы доверительных отношений

Существует два типа доверительных отношений между доменами: односторонние (one-way trust) и двусторонние (two-way trust).

- При односторонних пользователи только одного домена (доверяемого) имеют доступ к ресурсам другого (доверяющего).
- При двусторонних оба домена являются и доверяющими, и доверяемыми. У пользователей любого из доменов имеется доступ к ресурсам другого домена.

Между несколькими доменами могут устанавливаться множественные доверительные отношения. Например, несколько доменов могут доверять одному (в котором хранятся учетные записи всех пользователей), или один домен может доверять сразу нескольким доменам, при этом любые отношения доверия могут быть как двусторонними, так и односторонними.

В дальнейшем на рисунках доверительные отношения обозначаются стрелками. Домены, на которые они указывают, — доверяемые (в них хранятся учетные записи). А исходить стрелки будут от доверяющих доменов (в них находятся ресурсы). Образно говоря, стрелки указывают на "*людей*, которым можно доверять".

Доверительные отношения можно представить так. Допустим, Вы собрались в командировку, а дома у Вас цветы, которые надо поливать. Вы даёте соседу ключ от квартиры. В Ваше отсутствие он беспрепятственно входит к Вам в дом, поливает цветы, смотрит телевизор и т.п. Вы же лишены возможности без его разрешения попасть в его квартиру — своего-то ключа он Вам не давал!

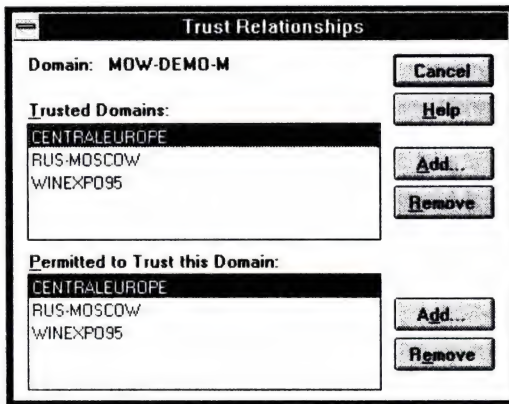
Но если сосед тоже часто бывает в отлучках, а дома у него кот, которого надо кормить, то ему ничего не остается, как дать ключ от своей квартиры Вам. И тогда Вы тоже сможете беспрепятственно входить в его квартиру. Это пример двусторонних отношений доверия. Строго говоря, пример не совсем корректен — ресурсы доверяющего домена доступны постоянно. (В рассмотренном примере — даже когда Вы дома и принимаете даму, а сосед врывается с лейкой в самый неподходящий момент.)

Роль доверительных отношений в сети чрезвычайно важна. Независимо от того, в каком месте сети он регистрируется, пользователь может указать не только свое имя, но и домен, к которому принадлежит. Так что он и доступ в сеть получит, и сохранит все привилегии и права, которыми обладает в своем домене.

Устанавливая доверительные отношения, сначала определите, где будут находиться учетные записи пользователей, — ведь пользователи, имеющие учетные записи в доверяемом домене, получают те же права и привилегии в доверяющем домене.

Так как доверительные отношения — в первую очередь средство администрирования учетных записей пользователей, определите *домен учетных записей* (account domain), а затем разрешите в нем другим доменам доверять ему.

Любой домен может инициировать установление доверительных отношений, но завершить установление можно только реализацией таких отношений в обоих доменах. Для этого предназначена команда **Trust Relationships** из меню **Policies** в **User Manager for Domains**.



Диалоговое окно Trust Relationships.

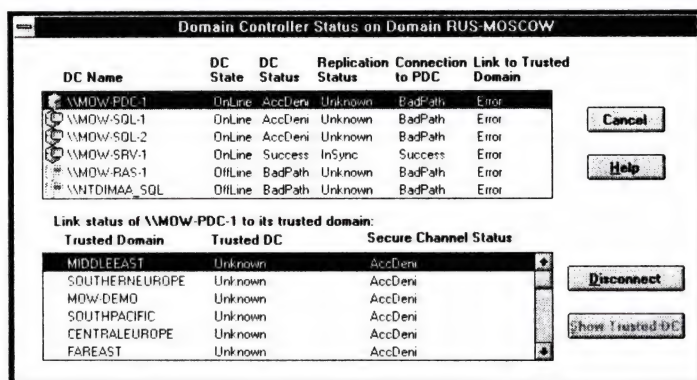
В изображенном на рисунке диалоговом окне два списка. В верхнем перечислены доверяемые домены, в нижнем — доверяющие. Домен MOW-DEMO-M является доверяющим для доменов CENTRALEUROPE, RUS-MOSCOW, WINEXPO95. Он же — доверяемый для тех же доменов. Следовательно, это двусторонние доверительные отношения.

На рисунке представлены примеры обоих типов доверительных отношений:



Администратор большой сети всегда должен иметь полную информацию о состоянии домена и его связей с другими. Ведь от того, как осуществляется синхронизация между базами учетных записей на контроллерах домена, и от возможности контроллера одного домена связаться с контроллерами доверяемых доменов зависит, насколько беспрепятственно пользователи будут осуществлять

доступ к ресурсам других доменов и регистрацию в них. Получить такую информацию поможет утилита **Domain Monitor** из Windows NT Resource Kit, позволяющая отслеживать состояние сразу нескольких доменов.



Диалоговое окно *Domain Controller Status*.

На приведенном рисунке показана достаточно критичная для функционирования системы ситуация. Хорошо видно, что часть резервных контроллеров домена уже не существует физически, но продолжает числиться в домене; с некоторыми контроллерами нет связи и наблюдается рассинхронизация; для многих доверяемых доменов даже неизвестно имя их PDC, а доступ к ним запрещен!

Типы доменных моделей

Между 2-3 доменами доверительные отношения организовать довольно просто. С ростом числа доменов и административных групп управление сетью усложняется. Поэтому существует четыре концептуальные модели доменных отношений: однодоменная, с одним мастер-доменом, с несколькими мастер-доменами и полностью доверительная.

Однодоменная модель

Модель с одним доменом подходит компаниям с небольшим числом пользователей и ресурсов. Поскольку домен только один, в доверительных отношениях нет необходимости. Администратор домена управляет всей сетью. Основные компоненты этой модели — пользователи и группы со своими ресурсами. Эта модель изображена на рисунке ниже.



Однодоменная модель.

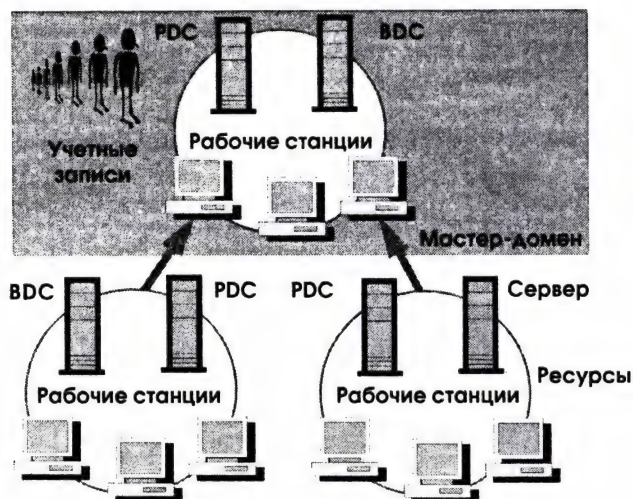
В таблице перечислены преимущества и недостатки однодоменной модели.

Преимущества	Недостатки
Лучшая модель для организаций с небольшим числом пользователей и ресурсов.	Низкая производительность, если в домене слишком много пользователей и групп.
Централизованное управление учетными записями пользователей.	Нет группирования пользователей по подразделениям.
Локальные группы определяются только один раз.	Нет группирования ресурсов.
Не нужно устанавливать доверительные отношения.	При большом числе серверов медленно выполняется просмотр сети.

Максимальное число учетных записей пользователей в одном домене — 40 000. Однако, планируя домен, следует учитывать, что максимальная нагрузка на один резервный контроллер домена — 2 000 учетных записей.

Модель с одним мастер-доменом

Эта модель удобна для тех фирм, где не требуется разделения на несколько доменов в организационных целях. Она позволяет осуществлять централизованное управление в сочетании с преимуществами использования нескольких доменов. На рисунке Вы видите схему модели с одним мастер-доменом:



Модель с одним мастер-доменом.

В этой модели всего один домен учетных записей. Учетными записями всех пользователей, находящимися в одном месте, управлять очень просто. Мастер-домен является доверяемым, а все остальные устанавливают с ним односторонние доверительные отношения. Поэтому пользователи, имеющие учетные записи в мастер-домене, получают доступ к ресурсам в доверяющих доменах, зарегистрировавшись в сети лишь один раз. В этой модели процесс администрирования делится на две части: администрирование учетных записей в мастер-домене и администрирование ресурсов во всех остальных доменах. Администратор может поручить администрирование ресурсов в одном из доверяющих доменов какому-либо лицу, чья рабочая станция входит в этот домен.

Данная модель наглядно демонстрирует двухъярусное построение домена. Мастер-домен принадлежит к первому ярусу, все остальные — ко второму.

Для упрощения администрирования доступа к ресурсам администратор должен создать глобальные группы в мастер-домене и включить их в соответствующие локальные группы в доверяющих доменах. Создав такие группы, администратору остается включить пользователя в ту или иную глобальную группу, чтобы обеспечить права на доступ к определенным ресурсам. (О группах см. раздел *Группы пользователей*.)

Модель с одним мастер-доменом наиболее приспособлена для:

- централизованного управления учетными записями (добавление, удаление и модификация учетных записей выполняются из одной точки);

- децентрализованного управления ресурсами или локального системного администрирования; домены подразделений могут иметь своих собственных администраторов, управляющих ресурсами подразделения;
- логической группировки ресурсов (ресурсы можно сгруппировать в соответствии с локальными доменами);
- сетей, в которых общее число учетных записей пользователей и групп не превышает 40 000.

При реализации этой модели придерживайтесь следующих рекомендаций:

- Число доменов второго яруса не должно быть большим. Поэтому не стоит автоматически включать небольшие офисы и подразделения в отдельный домен второго яруса. Лучше их включать в уже существующие домены.
- Модель с одним мастер-доменом предъявляет требования к расположению резервных контроллеров домена:
 - Если ресурсные домены подключены к домену учетных записей глобальными линиями связи, в ресурсном домене должен быть хотя бы один BDC для аутентификации пользователей этого домена в случае разрыва линии связи;
 - Если ресурсные домены находятся в той же локальной сети, что и домен учетных записей, то нет необходимости размещать в них BDC.

Ниже перечислены преимущества и недостатки рассмотренной модели.

Преимущества

Удобна для тех организаций, где относительно немного пользователей, а ресурсы нуждаются в группировке.

Глобальные группы определяются только один раз.

Ресурсы группируются локально.

Домены подразделений могут иметь собственных администраторов, управляющих ресурсами подразделений.

Централизованное управление учетными записями пользователей.

Поддержка до 40 000 учетных записей.

Недостатки

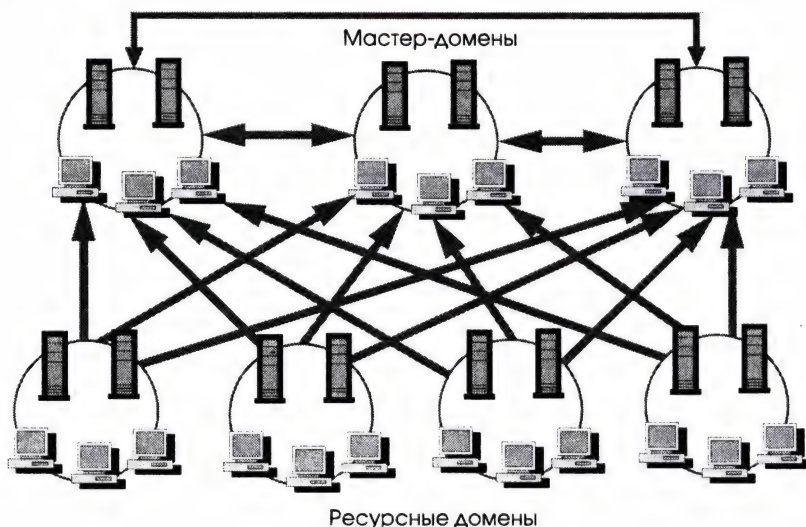
Низкая производительность, если в домене слишком много пользователей и групп.

Локальные группы необходимо определять в каждом из доменов, где они будут использоваться.

Модель с несколькими мастер-доменами

В этой модели используются два и более мастер-доменов. Аналогично тому, как это сделано в предыдущей модели, здесь мастер-домены являются доменами учетных записей. Каждый пользователь организации имеет учетную запись в одном из мастер-доменов. Администраторы системы могут централизованно управлять всеми учетными записями. Все остальные домены являются ресурсными — в них содержатся не учетные записи пользователей, а сгруппированные ресурсы, такие как принтеры и файл-серверы.

В этой модели каждый мастер-домен связан с другим двусторонними доверительными отношениями. Каждый ресурсный домен доверяет каждому мастер-домену и имеет с ним односторонние доверительные отношения. Так как учетная запись пользователя хранится в одном из доменов учетных записей, а между всеми доменами учетных записей установлены двусторонние доверительные отношения и все ресурсные домены доверяют мастер-доменам, пользователь получает доступ ко всем ресурсам организации. Схематично модель с несколькими мастер-доменами представлена на рисунке.



Модель с несколькими мастер-доменами. В этом примере на каждую учетную запись пользователя приходится одна учетная запись машины. Следовательно, в каждом из мастер-доменов может быть до 26 000 учетных записей пользователей.

Пользователи должны регистрироваться в домене, содержащем их учетные записи. В каждом мастер-домене должно быть не менее двух серверов, на которых происходит аутентификация пользователей.

В модели с несколькими мастер-доменами группы используются точно так же, как и в модели с одним мастер-доменом. Администраторы, создав глобальные группы в каждом из мастер-доменов, включают пользователей в те или иные глобальные группы. Затем глобальные группы включаются в различные локальные группы для обеспечения доступа к нужным ресурсам в доменах второго яруса.

В таблице перечислены преимущества и недостатки модели с несколькими мастер-доменами.

Преимущества**Недостатки**

Лучший выбор для компаний с большим числом пользователей и одним центральным офисом технического персонала.

Как локальные, так и глобальные группы необходимо определять несколько раз.

Масштабируемость на любое число пользователей.

Учетные записи пользователей не находятся в одном домене.

Ресурсы группируются логически.

Необходимо устанавливать большое количество доверительных отношений.

Домены подразделений могут иметь своих администраторов, управляющих ресурсами подразделения.

Мобильные пользователи могут быть зарегистрированы в любом месте сети.

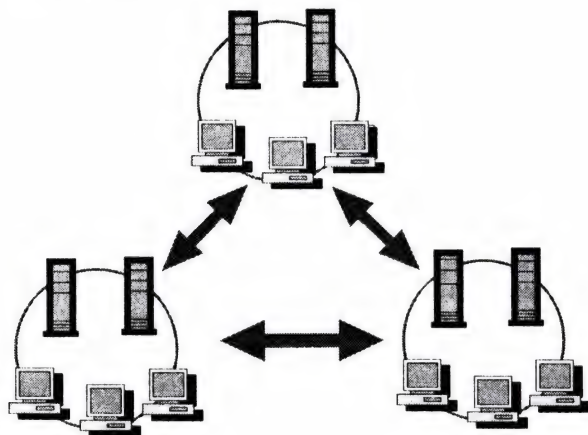
Поддержка более 40 000 учетных записей.

При реализации сети следует учесть те же требования к расположению и количеству резервных контроллеров домена, что и в случае с одним мастер-доменом:

- ▶ один BDC должен обслуживать не более 2 000 учетных записей;
- ▶ если ресурсный домен связан с доменами учетных записей через глобальную сеть, он должен иметь по крайней мере по 1 BDC для каждого из мастер-доменов.

Модель полностью доверительных отношений

Модель полностью доверительных отношений подходит для организаций с большими секторами, которые надо разбить на домены по отделам, и где нет централизованной технической службы. Это модель полностью децентрализованного управления:



Модель полностью доверительных отношений.

В модели полностью доверительных отношений администрирование пользователей и доменов распределено по подразделениям. Это удобно в организациях, где доменов немного, но с ростом их числа резко увеличивается количество доверительных отношений. Из-за децентрализации данная модель непригодна для организаций с централизованной технической службой.

Группы здесь используются так же, как и в модели с одним мастер-доменом. Администратор каждого из доменов определяет глобальные группы и включает в них пользователей. Затем он включает эти глобальные группы в локальные группы других доменов, чтобы предоставить доступ к ресурсам. Администратор должен определить и локальные группы и связать их с определенными ресурсами. Так что каждый из доменов является одновременно и ресурсным, и доменом учетных записей.

Благодаря двусторонним доверительным отношениям между доменами, зарегистрированный в своем домене пользователь имеет доступ к ресурсам и остальных доменов. Число доверительных отношений, устанавливаемых между n доменами, определяется по формуле: $n \times (n - 1)$. Так, для 10 доменов нужно $10 \times (10 - 1) = 90$

доверительных отношений. Добавление одного домена к 10 существующим требует установки 20 новых отношений доверия.

В таблице приведены преимущества и недостатки модели полностью доверительных отношений.

<i>Преимущества</i>	<i>Недостатки</i>
Подходит для компаний без централизованной технической службы.	Отсутствие централизованного управления не позволяет использовать эту модель в организациях с централизованной технической службой.
Масштабируется на любое число пользователей в сети.	Необходимо устанавливать очень большое число доверительных отношений.
Каждое подразделение имеет полный контроль над своими пользователями и ресурсами.	Каждый отдел зависит от другого в плане допуска пользователей в глобальные группы.
Как ресурсы, так и учетные записи пользователей сгруппированы по подразделениям.	
Масштабируются в сетях с числом пользователей, превышающим 40 000.	

Главный недостаток этой модели — слабость контроля за пользователями и группами в каждом из доменов. Поэтому применять ее не рекомендуется.

Практическая реализация доменных моделей

Познакомившись с описанием доменных моделей и, в частности, моделей с одним или несколькими мастер-доменами, Вы можете задать вопрос: “Что и где нужно указать в настройках Windows NT Server, чтобы объявить его контроллером *мастер-домена* или контроллером *ресурсного домена*?”

Подчеркнем: это чисто организационное деление. Нет никакой принципиальной разницы между первичными контроллерами этих доменов. Единственное отличие в том, что в мастер-доменах учетные записи пользователей и глобальные группы есть, а в ресурсных доменах их нет (но имеются локальные группы). Стоит Вам забыть и создать несколько учетных записей пользователей в ресурсном домене, как он перестанет быть чисто ресурсным, а администрирование сети несколько усложнится. Правда, как Вы увидите в дальнейшем, это не так страшно, как может показаться.

Гибкость использования разных моделей доменов в организациях

Имея несколько моделей организации доменов, Вы создадите гибкую и наращиваемую сеть, которая будет соответствовать меняющейся структуре компании. При этом используется исключительно Windows NT Server. В особенности удовлетворяются потребности:

- организаций с большим количеством филиалов;
- больших организаций;
- систем, в которых необходимо обеспечить защиту важной информации.

Расширить систему очень просто. Один домен в дальнейшем можно объединить с доменом другого офиса или связать с уже существующим большим доменом. Так как конкретная организация сети зависит от конкретного предприятия (его структуры, расположения, вида деятельности и т.п.), ниже представлены варианты организации доменов.

Предприятия с несколькими независимыми направлениями производства

Рассмотрим предприятие, занимающееся несколькими независимыми направлениями бизнеса, например: консалтингом, операциями с недвижимостью и розничной торговлей. В каждом из подразделений — свои группы маркетинга, продаж и обработки данных. Однако в центре предприятия есть небольшая группа, в задачи которой входит функциональное обслуживание, скажем, финансы, бухгалтерия и кадры.

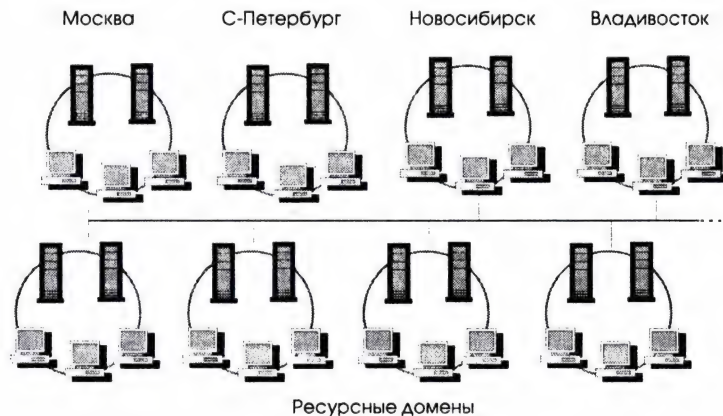
Чаще всего служащие одного подразделения используют ресурсы только своего подразделения (похоже на модель с одним мастер-доменом), однако иногда им (в особенности служащим центрального подразделения) нужен доступ к ресурсам другого подразделения, для чего требуется связь между мастер-доменами.



Модель с несколькими мастер-доменами на предприятии с несколькими независимыми линиями бизнеса.

Крупные предприятия

В данном примере рассмотрена очень большая организация с числом сотрудников, превышающим 100 000 человек, расположенных в нескольких местах. Используя модель с несколькими мастер-доменами, в каждый домен можно поместить до 26 000 пользователей. В соответствии с заданным сценарием надо создать не менее 4 мастер-доменов, каждый из которых будет содержать по 25 000 учетных записей пользователей и машин. Если же компьютеров гораздо меньше, число учетных записей пользователей в домене может достигать 40 000.

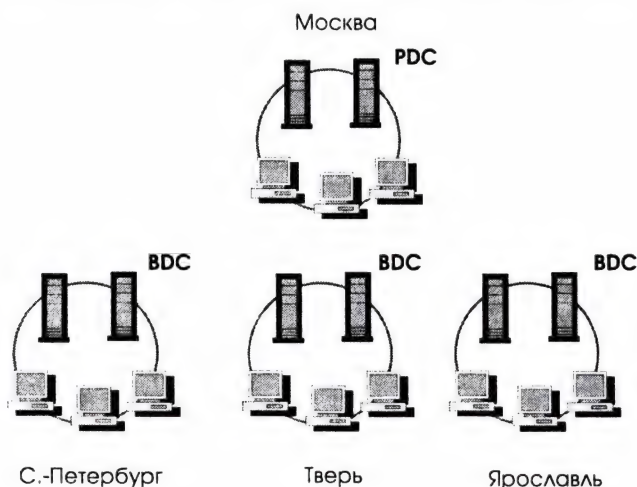


Модель с несколькими мастер-доменами на предприятии с числом сотрудников, превышающим 100 000.

Домены, в которых определены пользователи, могут разделяться по самым разным признакам: по алфавиту, секторам или физическому местоположению. Однако для пользователя это безразлично, так как между всеми мастер-доменами установлены двусторонние доверительные отношения.

Филиалы

В случае с филиалами можно задействовать как модель с одним доменом, так и модель с одним мастер-доменом. Предполагая, что PDC связан с филиалом посредством коммутируемой линии через модем или аналогичной линией связи, в каждом филиале необходим BDC. Резервный контроллер будет использоваться как для аутентификации локальных пользователей, так и в качестве сервера файлов и сервера печати. Для защиты от сбоев можно добавить и второй BDC.



Офисы в филиалах: соединение в рамках одного домена. В каждом филиале требуется один резервный контроллер домена.

Защищенные домены

В модели нескольких мастер-доменов между доменами учетных записей установлены двусторонние доверительные отношения, что предоставляет пользователям доступ к ресурсам всех доменов. Однако некоторые подразделения могут обладать конфиденциальной информацией (скажем, финансовыми записями, сведениями о кадрах и т.п.). Тогда вся организация может обслуживаться в рамках модели с одним мастер-доменом, а финансовое и кадровое подразделения выделяются в отдельные домены. Они доверяемы главным мастер-доменом, но не доверяют ему, т.е. пользователи финансового и кадрового домена имеют доступ к ресурсам предприятия, а пользователи предприятия доступа к ресурсам этих двух защищенных доменов лишены.



Защищенные домены: пользователи доменов финансового отдела и отдела кадров имеют доступ к ресурсам всего предприятия, однако сотрудники предприятия лишены доступа к ресурсам этих двух доменов.

Таким образом, выбор модели доменов зависит от числа пользователей и от того, как управляется предприятие. В таблице приведены рекомендации по выбору оптимальной модели доменов.

Атрибут домена	Одиночный домен	Один мастер-домен	Несколько мастер-доменов	Полностью доверительные отношения
Менее 40 000 пользователей в домене	✓	✓		
Более 40 000 пользователей в домене			✓	
Централизованное управление учетными записями	✓	✓	✓ ¹	
Централизованное управление ресурсами	✓			
Децентрализованное управление учетными записями			✓ ¹	✓
Децентрализованное управление ресурсами		✓	✓	✓
Центральная техническая служба	✓	✓	✓	
Отсутствие центральной технической службы				✓

¹ Модель с несколькими мастер-доменами позволяет осуществлять как централизованное, так и децентрализованное управление ресурсами.

Рекомендации по нагрузке доменов

Соотношение между числом рабочих станций и серверов в домене определяет скорость отклика во время регистрации пользователя в домене. Чем больше резервных контроллеров домена, тем больше пользователей одновременно регистрируются. Один BDC поддерживает до 2 000 учетных записей пользователей. Ниже в таблице приведено количество BDC в зависимости от числа пользователей. Данные рассчитаны, исходя из того, что в качестве BDC используются компьютеры с конфигурацией 486/66 с 32 Мб оперативной памяти.

<i>Число рабочих станций</i>	<i>Число серверов BDC</i>
10	1
100	1
500	1
1 000	1
2 000	1
5 000	2
10 000	5
20 000	10
30 000	15

При расчете учтено, что все точки расположения BDC связаны с первичным контроллером быстрыми линиями связи. Во многих организациях установку и конфигурирование BDC выполняют одновременно с установкой PDC, а после завершения синхронизации переносят в нужное место.

Выбирая тип компьютера для использования в качестве PDC или BDC, ориентируйтесь на данные, приведенные в таблице:

<i>Размер файла базы SAM</i>	<i>Число учетных записей пользователей¹</i>	<i>Минимально необходимый тип процессора</i>	<i>Требуемый объем оперативной памяти²</i>
5 Мб	до 3 000	486DX/33	32 Мб
10 Мб	7 500	486DX/66	32 Мб
15 Мб	10 000	Pentium, MIPS, Alpha AXP	48 Мб
20 Мб	15 000	Pentium, MIPS, Alpha AXP	64 Мб
30 Мб	20 000–30 000	Pentium, MIPS, Alpha AXP	128 Мб
40 Мб	30 000–40 000	Pentium, MIPS, Alpha AXP	166 Мб

¹ Число учетных записей пользователей указано приблизительно. Реально оно определяется совокупностью числа учетных записей пользователей, групп и компьютеров.

² Объем оперативной памяти должен быть минимум в 2,5 раза больше объема базы SAM.

Требования к серверу при установлении доверительных отношений

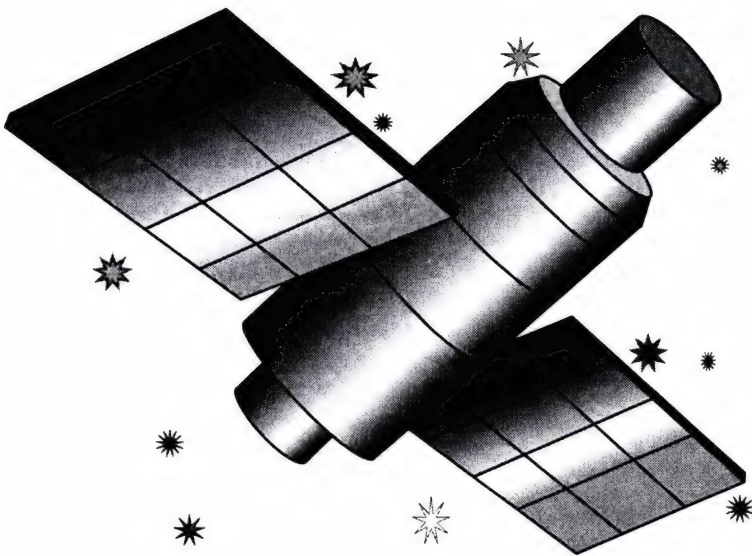
В Windows NT версии 3.5х максимальное *рекомендуемое* число доверительных отношений, которое можно установить с одним доменом, равно 128. (Заметьте: нигде нет такого параметра, как просто максимальное число доверительных отношений.)

4.0

- В Windows NT 4.0 служба каталогов NTDS позволяет использовать большее число доверительных отношений, и, надо отметить, это число может расти вместе с ростом объема оперативной памяти. В общем случае оно зависит от объема пула нестраничной памяти (non-paged pool — NPP).
- По умолчанию объем NPP зависит от объема памяти на сервере следующим образом:
- 32 Мб ОЗУ соответствует 1.2 Мб NPP (максимум 140 доверяемых доменов);
- 64 Мб ОЗУ соответствует 2.125 Мб NPP (максимум 250 доверяемых доменов);
- 128 Мб ОЗУ соответствует 4.125 Мб NPP (максимум 500 доверяемых доменов).
- Так как размер NPP может быть изменен администратором, то сервер с объемом оперативной памяти 64 Мб вполне будет способен поддерживать 500 доверительных отношений.

Планирование и установка системы

Театр начинается с вешалки, а операционная система — с установки. Перефразируя известную поговорку, можно сказать: как установишь, так и поработаешь. Так что прежде чем схватить коробку с NT Server и броситься его устанавливать, сначала как следует все спланируйте. Установка системы без предварительного определения типа компьютеров, протоколов и взаимоотношений равносильна потере номерка в толчее у театрального гардероба.



Планирование системы

Прежде чем приступить к планированию системы, стоит задуматься о главном: а что, собственно говоря, Вы желаете получить от своей сети? Какова цель затеваемой перестройки? Может, это просто дань моде, и Вы с парой сотрудников компании вполне справитесь с работой и без сети? Нет? Тогда будьте готовы ответить на такие вопросы:

- Сколько и каких компьютеров в Вашей организации?
- Используете ли Вы уже сеть?
- Как территориально расположены рабочие места?
- Какие задачи Вы решаете и собираетесь решать?
- Каковы взаимоотношения между подразделениями?
- Есть ли у Вас грамотные технические специалисты, способные обслуживать сеть?
- И т.д., и т.п.

Понятно, что Вы один не сможете ответить на все вопросы. Посоветуйтесь с сотрудниками, обратитесь к знакомым, которые уже прошли этот тернистый путь и могут предостеречь Вас от возможных ошибок.

Роль Windows NT Server в сети

Во Введении я уже перечислял функции, которые выполняет NT Server. Давайте "примерим" их теперь к своим задачам. Чтобы сделать правильный выбор типа и количества требуемой техники, а также определить необходимое число лицензий на программное обеспечение, заполним такую табличку:

Функция	Число пользователей	Используемые приложения	Объем дискового пространства	Примерный объем памяти
Файл-сервер				
Сервер печати				
Сервер приложений				
Сервер удаленного доступа				
Сервер вспомогательных служб				
Контроллер домена				
Сервер связи или эмуляции Netware Server				

Файл-сервер

Файл-сервер, как правило, нужен всем. Причем сегодня, когда стоимость жесткого диска объемом 1Гб такова, что его можно установить практически на каждом рабочем месте, ценность сервера файлов заключается только, пожалуй, в возможности организации эффективной работы коллектива над документами и в простоте контроля и управления персональными каталогами. Не надо думать, что сервер — файловая свалка, которую почему-то упорно называют файл-сервером.

Нет, возразят мне, файл сервер еще можно использовать для хранения одной копии какого-либо офисного продукта и запускать его с рабочих станций. А еще на нем можно хранить... базы данных. А еще... Постойте, не горячитесь. Так мы дойдем до того, что на нем можно жарить яичницу. Разберемся спокойно. Итак, Вы хотите запускать с сервера несерверные приложения (именно “несерверные” — ведь офисные продукты являются *персональными*)? Давайте рассмотрим несколько типичных ситуаций, о которых прошедшие через это рассказывали мне со слезами на глазах.

Ситуация первая: начало рабочего дня. Каждый пользователь включает компьютер и запускает с сервера свои офисные приложения. Их минимум 3: текстовый процессор, электронная таблица и персональная база данных. Нетрудно представить, как в это время будут перегружены и сеть, и сам сервер. Нужно обеспечить большой “запас прочности” сервера, чтобы он не “проседал” в пиковые моменты времени.

Ситуация вторая: администратор выключает сервер для профилактики. Несмотря на малую вероятность (кто среди рабочего дня выключит сервер?) такое случается довольно часто. Чего только не рассказывают “бывалые” о вредных уборщицах, всеядных тараканах, пьяных электриках и т.п., стремящихся всеми способами вывести сервер из строя! Что происходит, если пользователь, запустив Word с сервера, редактирует документ, также находящийся на сервере в момент выключения сервера? Правильно. Лексику, употребляемую в этот момент, лингвисты называют “ненормативной”.

Ситуация третья: Вы используете некоторую программу, написанную на Клиппере, Dbase или иной подобной системе доступа к данным путем их совместного использования (file sharing database). Данные конфиденциальны, и Вам хотелось бы, чтобы пользователи получали к ним доступ только через Вашу программу, которая по лишь ей ведомым правилам разграничивает доступ. Не выйдет! Либо Вы разрешаете пользователю работать ТОЛЬКО с Вашей программой и лишаете его остальных возможностей сети, либо Вы его полностью “отрезаете” от сервера с данными, но даете насладиться всеми прочими прелестями, придуманными той частью программистской братии, что не писала Вашу убогую программу. Чем раньше Вы перейдете на системы типа “клиент-сервер”, тем быстрее разрешите эту дилемму.

Вы продолжаете настаивать, что файл-сервер Вам нужен? Что ж, впишите в табличку, скольким пользователям он понадобится, каков объем общедоступных файлов, сколько мегабайтов Вы разрешаете иметь каждому пользователю и какие именно приложения они будут запускать с сервера.



Кстати: В Windows NT Server нет встроенной возможности квотирования жесткого диска (т.е. предоставления пользователям лимитированного объема). Это значит, что независимо от объема жесткий диск на сервере забивается "под завязку" уже через несколько дней, и только строгий административный контроль удержит пользователей от "синдрома Плюшкина".

Сервер печати

Серверы печати еще не утратили актуальности. Конечно, пока в большой сети гораздо дешевле поставить 1-2 высокоскоростных и высококачественных лазерных принтера и предоставить их в совместное использование, чем на каждое рабочее место — несметное число матричных, струйных или дешевых лазерных принтеров.

Однако, выбирая типы и количество принтеров, необходимо руководствоваться конкретными задачами. Скажем, принтеры, устанавливаемые в издательстве, отличаются от принтеров, обслуживающих бухгалтерию.

Планируя расположение и тип принтера, оцените количество пользователей, которые будут печатать на нем документы, средний объем и количество документов. Данные занесите в табличку.

Сервер приложений

Сервер приложений — это компьютер, на котором исполняются "тяжелые и мощные молотилки данных", способные в ответ на запрос, поступающий с клиентской рабочей станции, перерабатывать огромные массивы информации и передавать назад лишь результат. В описании серверных приложений налицо две составляющие: серверная и клиентская; поэтому они и называются приложениями типа клиент-сервер.



Кстати: Не стоит думать, что если Вы установили Word for Windows на сервер и запускаете его со своего рабочего места, то он превратился в клиент-серверное приложение. Ничуть не бывало. Он по-прежнему исполняется в памяти и процессором Вашего компьютера. Вся разница только в том, откуда берется исполняемый файл.

К приложениям типа клиент-сервер, работающим под управлением Windows NT Server, относятся приложения семейства Microsoft BackOffice: сервер управления базами данных Microsoft SQL Server, сервер информационного обмена Exchange Server, сервер управления системой Systems Management Server и плюс к большим и мини-компьютерам SNA Server. Кроме того, существует более 2000 приложений других фирм, таких как Lotus, Informix, Oracle, SAP, Platinum, Saros и др. К ним стоит приглядеться повнимательней.

Если Вы уже разработали свое или планируете покупку готового серверного приложения, занесите в таблицу количество сотрудников, которые будут *одно-временно* использовать его, ресурсы, необходимые для данного приложения, и общее количество серверных приложений.

Сервер удаленного доступа

Когда речь заходит о сервере удаленного доступа, в первую очередь подразумеваются мобильные пользователи, разъезжающие по необъятным просторам нашей страны с “ноутбуками” под мышкой и периодически “выходящие на связь” с родной конторой для передачи важных сведений и получения дальнейших указаний. “Идеалист, — скажете Вы, — где это Вы видели рядового российского командированного с «блокнотом» за 10 000\$?” Ладно, пусть будет филиал какого-нибудь “Зверь-банка” в Тютюшахтинске, имеющий на вооружении 1-2 персональных компьютера, — идет?

Как бы там ни было, и в том и в другом случае удаленный доступ вполне возможен. Занесите в табличку максимальное число клиентов, *одновременно* осуществляющих удаленный доступ к центральной сети, выделив около 1Мб оперативной памяти сервера на одного удаленного пользователя. А на полях не забудьте пометить, какие компьютеры (читай: операционные системы) имеются на удаленных станциях.

Но сервер удаленного доступа можно использовать и для связи филиалов между собой. Если перед Вами стоит такая задача, подумайте, есть ли у Вас выделенная линия или выход в X.25 или ISDN. Можно, конечно, обойтись и обычными коммутируемыми линиями, но без некоторого труда Вы эту рыбку не вытянете.

Сервер вспомогательных служб

Весьма расплывчатая категория, включающая в себя практически все, что не было перечислено выше. Например, такие сервисы, как DHCP, WINS, SNMP, DNS, UPS, Backup и массу других. Необходимость в использовании некоторых определяется протоколами, применяемыми в сети, других — степенью надежности системы, третьих — внешними условиями. Конкретные рекомендации дать трудно. В каждом случае откройте соответствующие разделы документации и внесите в табличку необходимые данные.

Контроллер домена

В главе *Доменная структура сети и взаимоотношения доменов* приведены конкретные рекомендации по нагрузочной способности контроллеров домена. К этим рекомендациям Вы обратитесь позже — когда приступите к выбору техники.

Пока просто запишите в таблицу количество пользователей в сети.

Сервер взаимодействия с Netware

О взаимодействии с сетевыми продуктами фирмы Novell имеет смысл говорить, если у Вас они уже используются. В противном случае об этом лучше даже не думать: как бы хорошо ни были исполнены средства сопряжения двух сетей, у Вас все равно будет *разнородная* сеть со всеми вытекающими...

Планируя установку или приобретение тех или иных сервисов, отметьте на полях таблицы версию Netware, с которой необходимо наладить дружественные отношения. Если это Netware 2.x или 3.x, можно использовать Windows NT Server версий 3.51 или 4.0. Если же Netware 4.x — полнота взаимодействия достигается только в NT Server версии 4.0 (подробнее см. главу *В одной сети с Netware*).

Итак, если Вы планируете предоставить клиентам сети Microsoft прозрачный доступ к ресурсам (файлам или принтерам) Netware, установите Gateway Service for Netware. Для его планирования запишите число сотрудников, которые будут одновременно использовать этот шлюз. Оно не должно превышать числа пользовательских лицензий для выбранного Netware сервера минус 2.

При решении обратной задачи, т.е. предоставлении клиентам Netware прозрачного доступа к серверу Windows NT, также укажите число сотрудников, которые будут одновременно использовать ресурсы NT.

Не устали? Тогда рассмотрим пример. Допустим, в Вашей организации 75 компьютеров. Сейчас часть сотрудников использует сеть Netware 3.12 на 50 лицензий. На сервере у них установлен Microsoft Office Professional и программа складского учета, написанная на Clipper, с которой работают 17 человек. На клиентских рабочих местах стоит Windows 3.11. Кроме того, в удаленном филиале, куда все данные передаются терминальной программой, установлен 1 компьютер.

Вы хотите заменить устаревшую программу складского учета на более современную и производительную, предоставить прямой доступ к этой программе удаленному филиалу, сделать это как можно дешевле и безболезненней и обеспечить возможность дальнейшего наращивания возможностей сети. Кроме того, на рабочих местах планируется установка Windows 95. А еще Вы желаете установить современную систему электронной почты. На первом этапе Вы не хотите отказываться от использования сервера Netware.

Одно из возможных решений — создать вторую сеть на базе Windows NT, интегрировать ее с существующей, разработать новое приложение складского учета, использующего Microsoft SQL Server, организовать сервер удаленного доступа. Какое-то время разработанная программа будет эксплуатироваться параллельно существующей в тестовом режиме 10 пользователями. Заполненная таблица будет выглядеть так:

<i>Функция</i>	<i>Число пользователей</i>	<i>Используемые приложения</i>	<i>Объем дискового пространства</i>	<i>Примерный объем памяти</i>
Файл-сервер	75	Microsoft Office Pro. Персональные каталоги (по 40 Мб на пользователя)	80 Мб 3 Гб	? ?
Сервер печати	75	средний размер документа	4 Мб 300 Мб	?
Сервер приложений	10	Microsoft SQL Server	100 Мб	32 Мб
	75	Microsoft Exchange Server	500 Мб	48 Мб
Сервер удаленного доступа	1			1 Мб
Сервер вспомогательных служб	?	?	?	?
Контроллер домена	75			32 Мб
Сервер связи или эмуляции	48	Gateway или		
Netware Server	75	FPNW		

Ни в коем случае не стоит думать, что все это надо сложить. А о том, как обрабатывать эти данные и чем заменить знаки вопроса, я расскажу ниже.

Выбор техники

В любом информационном проспекте, посвященном Windows NT Server, Вы прочтете, что для установки сервера минимально необходимы:

- ▶ компьютер с процессором 386, 486, Pentium, Alpha AXP, MIPS R44xx или PowerPC;
- ▶ 16 Мб оперативной памяти;
- ▶ 90 Мб на жестком диске.



Замечание: Windows NT Server 4.0 нельзя установить на компьютер с 386 процессором.

Однако не торопитесь хватать первую оказавшуюся в Вашем распоряжении машину, отвечающую перечисленным требованиям. Далеко не факт, что это то, что Вам нужно.

Во-первых, *минимальные* требования позволяют использовать компьютер как сервер файлов или печати только 5-10 клиентам.

Во-вторых, настоятельно не рекомендую ставить сервер на машину с 386 процессором.

В-третьих, далеко не на каждом компьютере Windows NT будет работать произвительно и устойчиво (если вообще будет). Недаром среди специалистов бытует мнение, что Windows NT — лучшая тестовая программа. Эта система “выловит” такие некорректно установленные параметры устройств, которых не заметят MS-DOS, Windows или Netware. Поэтому нормальная работа этих систем еще не значит, что на компьютере запустится Windows NT.

Так как же выбирать технику? Сначала найдите список совместимого оборудования (Hardware Compatibility List — HCL) для той версии сервера, которую Вы планируете установить. Он есть либо у счастливых владельцев легального продукта (так как входит в поставку), либо на ежемесячном CD-ROM издании Microsoft TechNet. Самый полный и точный список всегда находится на сервере Web Microsoft (www.microsoft.com): в нем около 3000 названий компьютеров, на которых работа Windows NT гарантирована.

Вполне возможно, что у Вас уже достаточно мощная техника и Вы не планируете новых закупок. Если она не входит в HCL, придется принять меры к тому, чтобы все компоненты Вашего компьютера были включены в список совместимого оборудования. В нашей стране, изобилующей компьютерами сомнительного или даже “наколенного” происхождения, такое требование может показаться чрезмерным, но никуда не денешься — Вы рискуете не установить систему из-за отсутствия или неполной совместимости драйвера какого-нибудь устройства.

Какому же типу компьютера отдать предпочтение? Используйте только технику, “имеющую имя” (brand-name) и перечисленную в HCL, — это не дань моде и не “сговор с поставщиками”: производительность и надежность таких систем гораздо выше, чем у “безымянных”. Кроме того, Вам всегда предоставят техническую поддержку.

Существуют ли дополнительные рекомендации по выбору отдельных устройств компьютера, кроме обязательности их наличия в HCL? Могу посоветовать следующее:

Жесткий диск должен быть достаточно быстрым, желательно SCSI-диск. Это отнюдь не означает, что IDE-диски не поддерживаются в Windows NT. Просто SCSI-устройства гораздо проще в конфигурировании, у них выше производительность, кроме того, они предоставляют некоторые дополнительные возможности, повышающие надежность работы (см. главу *Обеспечение отказоустойчивости*).

Не экономьте на **сетевой плате**. Поставив какой-нибудь дешевый клон NE2000, Вы загубите производительность сервера. Такие устройства допустимы на рабочих станциях, но не на сервере. Почитайте, какие сетевые адаптеры используются в серверах Compaq, Dell, IBM, HP, и выберите подобный. Планируя удаленную загрузку с сервера бездисковых рабочих станций, позаботьтесь о том, чтобы BOOT ROM (ПЗУ загрузки) поддерживало режим работы с Microsoft Lan Manager, а не Novell Netware.

Проигрыватель компакт-дисков (CD-ROM) — обязательный атрибут NT Server. Сама система поставляется только на компакт-дисках, практически все серверные приложения также записаны на CD (Microsoft BackOffice, например, записан на 4 дисках). Практически все современные проигрыватели поддерживаются в Windows NT, но предпочтение стоит отдать либо SCSI-, либо IDE ATAPI-устройствам. При установке они опознаются автоматически, тогда как ранее популярные CD-ROM фирм Panasonic, Sony и др. надо указывать вручную. Желательно использовать четырех- или шестискоростные устройства.

В случае установки NT Server выбор **видеоадаптера** не важен. Помните лишь, что раритеты вроде CGA, EGA и Hercules системой вообще не поддерживаются. Windows NT работает с любым (или лучшим) VGA-адаптером. Даже если для выбранного типа не найдется драйвер, система будет работать в стандартном VGA-режиме 640 x 480.

Выбор необходимого объема оперативной памяти

Объем оперативной памяти — ключевой фактор, влияющий на производительность системы. Выбирая объем, руководствуйтесь принципом “чем больше, тем лучше”. Дело в том, что Windows NT хранит максимально возможное число открытых файлов в памяти, а за всеми остальными обращается к диску. Увеличение объема памяти оказывает на производительность даже большее влияние, чем замена процессора. Данная таблица позволяет примерно рассчитать необходимую величину.

Формула для вычисления объема оперативной памяти			Всего RAM
Факторы			
Память системы	Минимально необходимо 16 Мб	А <input type="text"/>	А
Данные пользователей	Средний объем файлов, открываемых каждым пользователем Число пользователей Умножить Б на В	Б <input type="text"/>	Г
		В <input type="text"/>	
		Г <input type="text"/>	
Приложения	Средний размер файлов, исполняемых на сервере Число приложений, выполняемых на сервере Умножить Д на Е	Д <input type="text"/>	Ж
		Е <input type="text"/>	
		Ж <input type="text"/>	
Общий рекомендуемый объем памяти:			А+Г+Ж

Вернемся к нашему примеру и рассчитаем необходимый объем оперативной памяти.

Поскольку планируется использовать одновременно Microsoft Exchange Server и Microsoft SQL Server, то, исходя из минимальных требований, получим $A = 48 \text{ Мб} + 32 \text{ Мб} = 80 \text{ Мб}$. Помимо этого этот же самый компьютер будет работать как сервер файлов и печати. Рассчитаем средний объем файлов, открываемых каждым пользователем.

Для Word for Windows — 310 Кб;

для Excel — 60 Кб;

для PowerPoint — 1000 Кб;

для Access — 500 Кб.

Средний объем (Б) = 685 Кб. Умножив его на число пользователей (75), получим $\Gamma = 51,4 \text{ Мб}$

Теперь рассчитаем объем памяти, необходимый для запуска с сервера приложений, входящих в Microsoft Office.

Для Word for Windows — 3,66 Мб;

для Excel — 4,6 Мб;

для PowerPoint — 4,16 Мб;

для Access — 2,7 Мб.

Средний объем равен 3,78 Мб. Таким образом, для запуска 4 приложений в среднем необходимо $3,78 \times 4 = 15,1 \text{ Мб}$ (Ж).

Сумма $A+\Gamma+Ж = 80 + 51,4 + 15,1 = 146,5 \text{ Мб}$.

При расчете я умолчал о том, что компьютер должен также работать в качестве сервера доступа к Netware и эмуляции функций Netware. Это необходимо было бы учитывать, только если бы были добавлены еще пользователи. Но если их количество неизменно, требования к памяти уже учтены параметром Г, независимо от используемого ими файлового сервиса.

Определение объема жесткого диска

При планировании объема жесткого диска рекомендуется использовать 3 логических раздела. Первый — для установки системы, второй — для приложений, устанавливаемых на сервере, третий — для персональных каталогов пользователей. Кроме того, советую иметь минимум 2 жестких диска. На одном из них должна быть установлена система Windows NT и файлы приложений, а на другом разместить файл подкачки. Это позволит значительно повысить производительность системы.

Когда к надежности системы предъявляются повышенные требования, количество жестких дисков и их общий объем нужно значительно увеличить для организации зеркализации дисков или массива дисков RAID (см. главу *Обеспечение отказоустойчивости*).

Для расчета объема жесткого диска используется следующая таблица:

Формула для вычисления объема жесткого диска			
Факторы			Всего (Мб)
Системный диск С:	Более 250 Мб или	А	А
	150 Мб + оперативная память + 12 Мб		
Диск приложений D:	Объем, занимаемый каждым приложением	Б	Г
	Число приложений, выполняемых на сервере	В	
	Умножить Б на В	Г	
Диск пользователей E:	Объем, отводимый под каждого пользователя	Д	Ж
	Число пользователей	Е	
	Умножить Д на Е и на 110% (погрешность)	Ж	
Общий рекомендуемый объем диска:			А+Г+Ж

Рассчитаем объем жесткого диска для нашего примера.

Пространство, отводимое под систему, $A = 150 \text{ Мб} + 146,5 \text{ Мб} + 12 \text{ Мб} = 308,5 \text{ Мб}$

Объем, занимаемый исполняемыми приложениями:

Microsoft Office — 80 Мб;

Microsoft SQL Server. Ранее в таблицу было записано 100 Мб;

Microsoft Exchange Server — 500 Мб (с учетом персональных почтовых ящиков);

под файл спулинга печати — 300 Мб.

Итого: $G = 780 \text{ Мб}$.

Объем, отводимый под пользователей. Ранее на каждого пользователя было выделено 40 Мб. Поэтому всего пользователям отводится $Ж = 40 \text{ Мб} \times 75 \times 1,1 = 3\,300 \text{ Мб}$.

Суммарный объем жесткого диска: $A+G+Ж = 308,5 + 780 + 3\,300 = 4\,388,5 \text{ Мб}$.

Если будет применяться зеркализация дисков, объем придется удвоить.

Выбор файловой системы

На сервере необходимо использовать NTFS, поскольку только эта файловая система обеспечивает защищенный доступ к файлам и возможность быстрого самовосстановления в случае краха системы. (Подробно о файловых системах см. главу *Файловая система NTFS*.) Однако при использовании RISC-системы необходимо оставить небольшой (примерно 2 Мб) загрузочный раздел в формате FAT. Если Вы предъявляете к защищенности своей системы повышенные требования, защитите доступ к этому разделу средствами BIOS компьютера.

Иногда полезно и саму систему установить на раздел FAT. Тогда даже при серьезном повреждении загрузочного диска, Вы сможете, загрузившись с дискеты с MS-DOS, попытаться его восстановить. Однако такая установка резко снижает защищенность системы в целом.

Выбор процессора

Мы уже говорили, что Windows NT поддерживает работу на разных типах процессоров. В каждом конкретном случае руководствуйтесь как текущей нагрузкой, так и нагрузкой, которая может возникнуть в будущем. Если Вы знаете, что в скором времени количество пользователей существенно увеличится или возрастет объем производимых вычислений, то сразу ориентируйтесь на приобретение компьютера, позволяющего установить более 1 процессора.

Если Вы хотите запускать на сервере MS-DOS-приложения, предпочтение стоит отдать Intel-процессорам.

В нашем примере компьютер должен выполнять функции:

- сервера файлов и печати;
- контроллера домена;
- сервера "тяжелых" приложений SQL Server и Exchange Server;
- сервера удаленного доступа;
- шлюза в сеть Netware и эмулировать работу сервера Netware.

Для одного процессора это тяжеловато. Но и Microsoft SQL Server, и Exchange Server хорошо используют возможности масштабирования Windows NT. Поэтому смело можно заложиться на 2-3 процессора в компьютере. Так как на сервере не планируется работа с MS-DOS-приложениями, это могут быть как Pentium (для Windows NT версии 4 лучше использовать Pentium Pro), так и другие (скажем, Alpha AXP) процессоры. Выбирая тактовую частоту руководствуются тем же принципом, что и при выборе памяти, но в нашем случае вполне хватит Pentium 90.

Альтернатива увеличения числа процессоров — несколько серверов, выполняющих различную функциональную нагрузку. Например, в нашем примере можно использовать 3 разных компьютера:

один — сервер файлов, печати, главный контроллер домена, сервер удаленного доступа, плюс в Netware и имитатор сервера Netware;

другой — сервер управления базами данных и резервный контроллер домена;

и третий — информационный сервер плюс резервный контроллер домена.

Кстати, использование нескольких серверов позволяет сделать несколько контроллеров домена, что обеспечивает бесперебойную работу.

Для нашего примера приведем две (из многих возможных) конфигурации:

	<i>С одним компьютером</i>	<i>С тремя компьютерами</i>		
Процессор	2 × Pentium 120	Pentium 90	Pentium 90	Pentium 90
ОЗУ	192 Мб	96 Мб	48 Мб	48 Мб
Объем на жестком диске	2 × 5 Гб	2 × 3 Гб	400 Мб	1 Гб
Функция	все	все, кроме СУБД и информ. обмена	СУБД, резервный контроллер домена	Информационный обмен, резервный контроллер

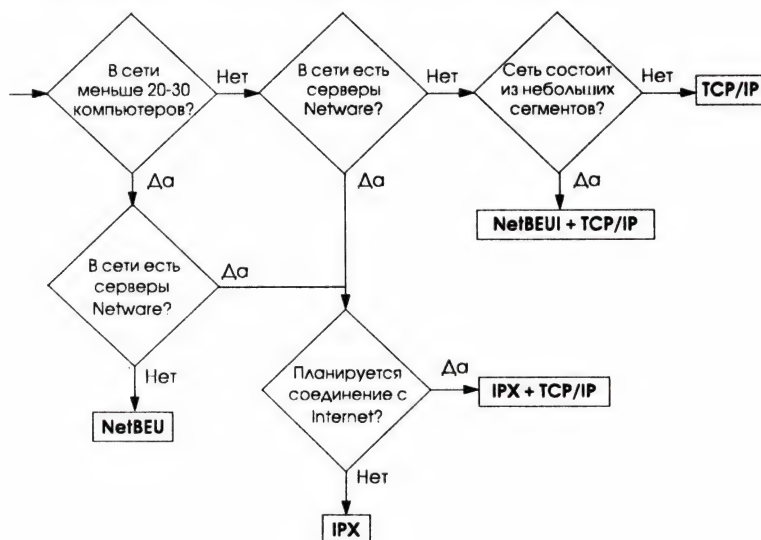
Отметим, что наш пример — частный случай и приведенную выше табличку нельзя рассматривать как догму. Помните: в каждом конкретном случае конфигурация будет в большой степени зависеть от числа пользователей, выполняемых ими задач, требований по безопасности системы и... Ваших финансовых возможностей. Хотя, если честно, последний фактор должен оказывать минимальное влияние.

Выбор сетевых протоколов

В Windows NT Server стандартно поддерживаются 3 сетевых протокола: TCP/IP, IPX/SPX и NetBEUI. Какому (каким) отдать предпочтение? Все зависит от условий работы. Для небольших сетей (до 20-30 компьютеров) подойдет NetBEUI, как самый быстрый. Правда, если в этой же сети есть серверы Netware, этот протокол бесполезен, и ему следует предпочесть IPX. В сетях, состоящих из небольших по размеру сегментов, соединенных через маршрутизатор (в роли которого может выступать NT Server), эффективно применение двух протоколов: NetBEUI и TCP/IP. Первый обеспечит наивысшую производительность внутри сегментов, а второй — связь между сегментами.

Если Вы вынуждены использовать протокол IPX и Вам нужен доступ в Internet, используйте и IPX, и TCP/IP.

Эта диаграмма поможет сделать правильный выбор.



На первый взгляд, в нашем примере целесообразнее использовать только IPX. По завершении использования Netware сеть должна быть переведена на работу с TCP/IP. Учитывая, что уже сегодня большая часть пользователей сможет осуществлять доступ к ресурсам Netware через шлюз, можно использовать TCP/IP на большинстве компьютеров, а IPX оставить лишь на некоторых в качестве второго протокола (например, на том сервере NT, который будет выполнять роль шлюза).

Приведенная диаграмма не охватывает еще два возможных случая: использование принтеров, подключаемых непосредственно к локальной сети, и работа с компьютерами Machintosh.

Принтеры можно подключить с использованием двух протоколов: TCP/IP или DLC. Второй протокол также входит в поставку NT Server, и после его установки все подключенные принтеры становятся доступны с сервера.

Если в Вашей сети есть компьютеры Machintosh, то чтобы использовать их как серверы файлов и печати Windows NT Server, дополнительно установите протокол Apple Talk, входящий в стандартную поставку.

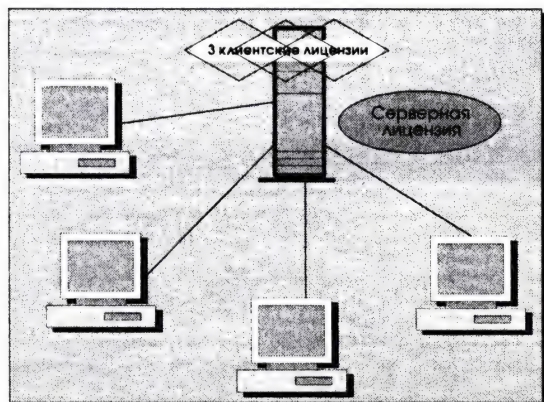
Планирование клиентских лицензий

Каждая фирма-производитель программного обеспечения ведет свою *лицензионную политику*, т.е. отслеживает легальность использования ее продукции. Политика фирмы Microsoft основана на том, что каждый пользователь, работая только с лицензионно чистыми продуктами, не применяет никаких средств *физического* ограничения возможностей работы с программами. Это значит, например, что, установив один Windows NT Server, Вы можете *физически* подключить к нему неограниченное число пользователей. Однако *легально* с сервером смогут работать лишь столько клиентов, сколько *клиентских лицензий* Вы приобрели. (Версии серверов Microsoft BackOffice, входящих в поставку Microsoft Development Network — MSDN, имеют физическое ограничение в 5 пользователей, так как предназначены исключительно для целей тестирования разработчиками своих программ.)

Лицензионная политика Microsoft весьма гибка и подходит для любого покупателя. Приобретая Windows NT Server, Вы покупаете не сам сервер, а только *лицензию на его использование*. Для установки Windows NT (или любого программного продукта Microsoft) на несколько компьютеров, хватит одной коробки с сервером, а для других компьютеров просто докупите *серверные лицензии*.

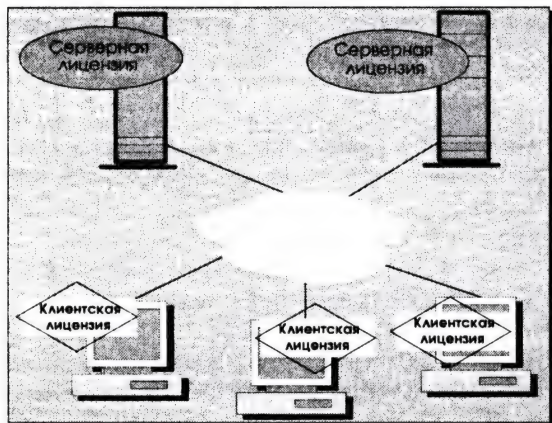
Теперь разберемся с клиентами. Существует два типа клиентских лицензий: *хранящаяся на сервере* (per-server license) и *хранящаяся на клиенте* (per-seat license). Понятие “места хранения” условно и определяется только тем, что Вы установите в диспетчере лицензий (License Manager). В чем их различие?

Если лицензии **хранятся на сервере**, то *одновременно* ресурсы этого сервера доступны такому количеству пользователей, которое *не превышает* числа хранящихся на этом сервере лицензий. Например, в Вашей сети 50 компьютеров, а Вы приобрели 40 клиентских лицензий и храните их на сервере. В этом случае легальным считается одновременное подключение к серверу до 40 клиентов. Клиенты могут быть любыми из имеющихся у Вас.



Хранение лицензий на сервере.

Если лицензии **хранятся на клиентах**, то ресурсами *любого сервера* в сети могут воспользоваться только клиенты, имеющие лицензию. Например, у Вас три Windows NT Server и 50 рабочих станций, на каждой из которых хранится клиентская лицензия. В таком случае можно осуществлять доступ с любого рабочего места к ресурсам любого из этих трех серверов (или даже ко всем трем сразу).



Хранение лицензий на клиентах.

Какой тип лицензии выбрать? Если у Вас только один сервер, к которому временно осуществляет доступ лишь часть клиентов, выгоднее использовать лицензии, хранящиеся на сервере. В остальных случаях выгоднее приобрести лицензии, хранящиеся на клиентах. А если сегодня в сети только один сервер, но через несколько месяцев их будет несколько? Купите лицензии типа per-server, а с появлением дополнительных серверов Вы *меняете* статус лицензии на per-seat. Лицензионная политика позволяет *однократно* выполнить такой переход.



Замечание: То, что Вы легальный владелец программного продукта, предоставляющего физический доступ к серверу, не значит, что Вы обладаете лицензией на доступ. Лицензия *всегда* приобретается дополнительно. Например, владелец Windows 95 или Windows NT Workstation обязан купить лицензию на право доступа к NT Server.



Выбор модели хранения клиентских лицензий.

Windows NT Server — это лишь один сервер из семейства серверных продуктов Microsoft BackOffice, и наличие серверных и клиентских лицензий для доступа к его ресурсам не дает оснований полагать, что Вы имеете лицензии на доступ к другим серверным продуктам. Они требуют *покупки своих собственных лицензий*. А как поступить, если Вы установили на компьютер NT Server + SQL Server?

Ответ зависит от того, как этот сервер будет использоваться. Возможно несколько сценариев.

Сценарий использования

Приобретаемые лицензии

Сервер используется как файл-сервер, и/или сервер печати, и/или сервер удаленного доступа ПЛЮС как сервер управления базами данных для пользователей локальной сети.

NT Server — серверная
SQL Server — серверная
NT Server — клиентские
SQL Server — клиентские

Сервер используется только как сервер управления базами данных в локальной сети.

NT Server — серверная
SQL Server — серверная
SQL Server — клиентские

Используется только SQL Server, выполняющий только роль хранилища данных для других серверных приложений (например, Systems Management Server или Internet Information Server).

NT Server — серверная
SQL Server — серверная
SQL Server — клиентские
по числу серверных приложений, использующих его

Таким образом, Вы покупаете лишь те лицензии, что реально будете использовать.

Кроме лицензий, отдельных для каждого серверного продукта, существует еще одна объединенная лицензия — на BackOffice, также имеющая две разновидности — серверную и клиентскую. Это приобретение выгодно при покупке трех и более серверов данного семейства. Учтите, однако, что она дает Вам право установить серверные программы *на один компьютер*. В результате наших расчетов было предложено либо на один компьютер с двумя процессорами установить NT Server, SQL Server и Exchange Server, либо на трех компьютерах установить по отдельному серверу. В первом случае выгоднее приобрести 1 серверную лицензию на BackOffice и 75 клиентских, а во втором — придется купить 3 серверные лицензии на NT Server, по одной серверной — на SQL Server и Exchange Server, по 75 клиентских — для NT Server и Exchange Server и 10 клиентских лицензий для SQL Server. Посчитав суммарную стоимость одной "навороченной" машины со стоимостью лицензий, Вы увидите, что она гораздо ниже стоимости использования тех же продуктов на 3 компьютерах попроще.

Процедура установки

Если Вы вняли дружеским советам, приведенным в начале главы, и выбрали технику, отвечающую всем необходимым критериям, процедура установки системы пройдет гладко и незаметно. В противном случае, придется заняться тем, что в кругу специалистов называется "шаманством" — битьем в бубен, танцами у костра и заклинаниями.

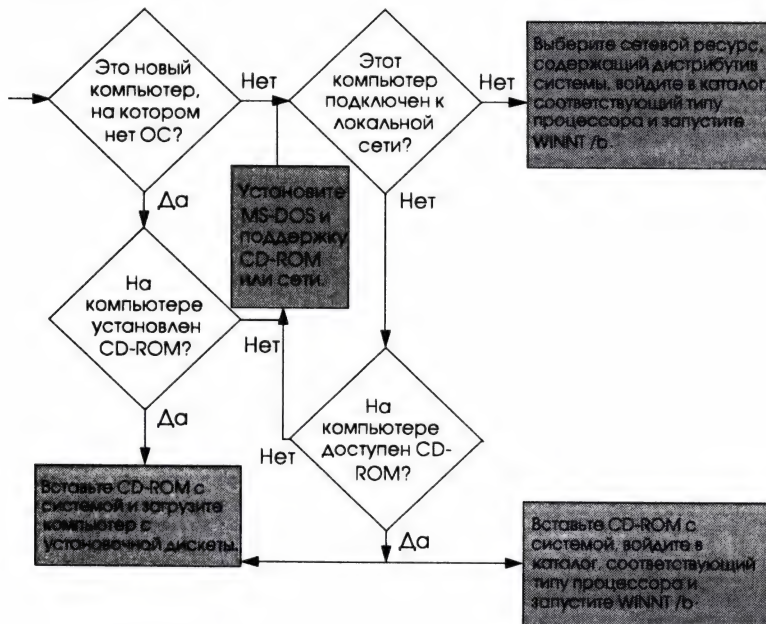
Итак, прежде всего:

1. Проверьте типы и параметры всех установленных систем: SCSI-адаптеров, сетевой платы, жестких дисков, проигрывателей компакт-дисков. Посмотрите и установки, записанные в CMOS-память компьютера; в старших областях памяти не должно быть никаких областей, зарезервированных под системное использование. Посмотрите, сколько процессоров реально установлено на главной плате.
2. Если Вы используете устройства типа SCSI, убедитесь, что на последнем из них установлены терминирующие резисторы, а соответствующая функция активизирована на SCSI-адаптере. Проследите за тем, чтобы ID этих устройств не совпадали.
3. Убедитесь, что IRQ и адреса, используемые различными устройствами, не совпадают и не перекрываются.
4. Если Вы хотите использовать несколько сетевых плат, сконфигурируйте их так, чтобы они не конфликтовали ни друг с другом, ни с прочими устройствами.
5. Если какие-либо устройства стандартно не поддерживаются в Windows NT, подготовьте дискеты с драйверами фирм-изготовителей.

Выбор способа установки

После всех подготовительных процедур можно приступить непосредственно к установке, которую можно выполнить разными способами в зависимости от конкретных обстоятельств. Можно выполнять установку, загрузив компьютер с дискет, можно начать ее с жесткого или с компакт-диска, а можно подключить компьютер к локальной сети и установить систему с сетевого диска. Какой из способов предпочесть, подскажет приведенная схема. Схема носит рекомендательный характер, так как, во-первых, отражает только установку на компьютеры с процессорами Intel, а во-вторых, Вы сами можете в конкретной ситуации выбрать подходящий способ.

Если выбрана команда **winnt /b**, сначала копируются все файлы, требуемые для установки системы на данном типе процессора из каталога-оригинала на жесткий диск. Позаботьтесь, чтобы перед установкой на нем было минимум 100 Мб свободного пространства (или 200 Мб, если Вы устанавливаете систему на диск C). Окончив копирование, система перезагрузит компьютер и начнет исполнение программы **Setup**.



Неграфическая часть установки

Программа установки имеет два режима — **Express** или **Custom**. Последний предпочтительнее, так как позволяет контролировать ряд параметров.

В начале установки происходит определение типов устройств, установленных в компьютере. Затем на экран выводится список обнаруженных SCSI-устройств. Если какое-то из установленных устройств не обнаружено или определено неправильно, нажмите клавишу **S** и выберите его из списка вручную.

Если же после принудительного указания типа устройства система сообщает о невозможности его инициализации, прервите программу установки и проверьте параметры оборудования. Вероятнее всего, это конфликт с другими устройствами.

Если установленного в системе устройства в списке нет, но у Вас есть его драйвер, выберите в списке «**Other**», вставьте дискету с нужным драйвером и установите его.



Кстати: Проигрыватели компакт-дисков рассматриваются как SCSI-устройства. Поэтому убедитесь, что программа установки определила Ваше устройство.



- Популярные в прошлом проигрыватели компакт-дисков типа Mitsumi,
- Panasonic и Sony, подключающиеся через свой собственный интерфейс,
- больше не входят в список стандартно поддерживаемых устройств. Необходимые для их работы драйверы лежат в каталоге DRVLIB на компакт-диске.

Следующий момент — выбор диска для установки системы. Как установить Windows NT на раздел, объем которого превышает 4 Гб? Если этот раздел уже имеет формат NTFS (скажем, подготовлен на другом компьютере), такого вопроса не возникает; если же еще нет, то во время установки он будет первоначально отформатирован как FAT, а значит (в силу ограничений FAT), не сможет быть большим. Ничего страшного: установив систему, воспользуйтесь программой **Disk Administrator** для увеличения объема тома.

Прежде чем начать копировать файлы в указанный Вами каталог, программа установки выведет список некоторых общих характеристик Вашего компьютера, таких как тип компьютера, тип клавиатуры и мыши. Не спешите машинально нажать Enter. Если вдруг Вы заметите, что система нашла несколько процессоров, а у Вас в машине реально установлен только один из нескольких возможных, замените тип компьютера на **Standard PC**.

Еще одно предупреждение — не указывайте в данной части программы установки русскую раскладку клавиатуры, иначе в дальнейшем Вам придется туго.

Неграфическая часть программы установки завершится копированием файлов, после чего будет предложено выполнить перезагрузку системы для продолжения установки.

Графическая часть установки

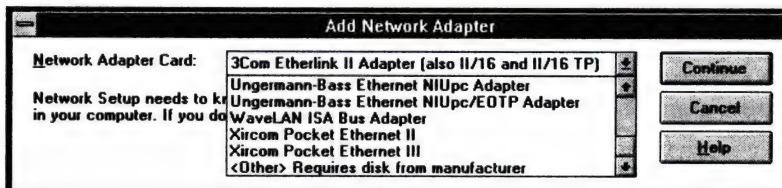
Графическая часть программы установки интуитивно понятна и не таит подводных камней, однако есть ряд моментов, на которые стоит обратить внимание.

1. Программа предложит выбрать текущие национальные установки (**Current Locale**). Обязательно установите **Russia**, если Вы надеетесь использовать русские системные шрифты. В работающей системе установить новые шрифты будет не так просто.

4.0

- Программа установки Windows NT Server 4.0 существенно отличается от предыдущей версии. В ней не будет предложено указать национальные параметры, так как их всегда можно с легкостью модифицировать в уже установленной системе.
2. На этапе **выбора сетевых плат** будьте особенно внимательны. Если Вы не укажете никакого сетевого устройства (а это может быть либо сетевая плата, либо сервис удаленного доступа), или укажете неверные параметры, установка Windows NT Server не сможет быть завершена. Для Windows NT Workstation это не так — данная система может быть установлена даже при отсутствии сетевого устройства.

Обычно тип сетевой платы и ее параметры опознаются автоматически, после чего будут предложены некоторые параметры конфигурации, которые можно либо принять, либо изменить. Изменять эти параметры имеет смысл, только когда программа установки сообщит о конфликтах между выбранными значениями и конфигурацией других устройств в системе.



Диалоговое окно Add Network Adapter.

Если установленное устройство стандартно не поддерживается операционной системой, но у Вас есть драйвер от производителя, выберите в списке **«Other»** и установите драйвер с дискеты.



Замечание: Если в компьютере более одной сетевой платы, то после определения первой нажмите кнопку *Next* для запуска процедуры определения следующей.

3. Программа предложила Вам выбрать **роль, которую будет играть сервер в домене**: сервер (server) или контроллер домена (domain controller). Увы, большинство допускает здесь ошибку (может, испугавшись непривычного слова "домен") и выбирает "сервер", даже если это вообще единственный сервер в сети Microsoft.

Прочитав эту книгу, Вы поймете, что только контроллер домена полноценно управляет сетью.

Итак, если устанавливаемый сервер является первым сервером Windows NT в сети, он должен быть главным контроллером домена.

Если это не первый сервер, он может быть как резервным контроллером домена, так и просто сервером. Что выбрать? В большинстве случаев желательно указать контроллер домена, иначе Вы лишитесь возможности централизованно управлять пользователями и ресурсами сервера.



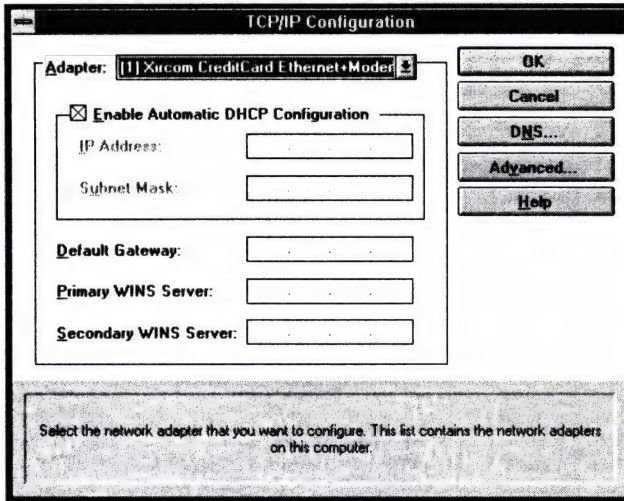
Замечание: Если Вы установите просто сервер, а затем захотите изменить его роль на контроллер домена, это можно будет сделать, только полностью переустановив систему.

Устанавливая резервный контроллер домена, помните:

- компьютер должен быть подключен к локальной сети, первичный контроллер домена в которой должен быть доступен;
- Вы должны знать имя учетной записи администратора и пароль, которые необходимы для включения нового компьютера в домен.

При установке **сетевых протоколов** выберите только нужные Вам протоколы. Далее определите их начальную конфигурацию.

Для протокола TCP/IP предлагается возможность выбора: задать либо фиксированный IP-адрес машины, либо автоматическое определение адреса механизмом DHCP. Какому способу отдать предпочтение?



Диалоговое окно TCP/IP configuration.

Для единственного сервера Windows NT в Вашей сети надо задать фиксированный адрес, потому что DHCP сервера не существует. Этот адрес можно задать произвольно, если Вы знаете, что доступ в Internet не планируется. Если же доступ в Internet является условием работы Вашей сети, то корректный адрес (или ряд адресов) Вы получите у компании, предоставляющей доступ в Internet.

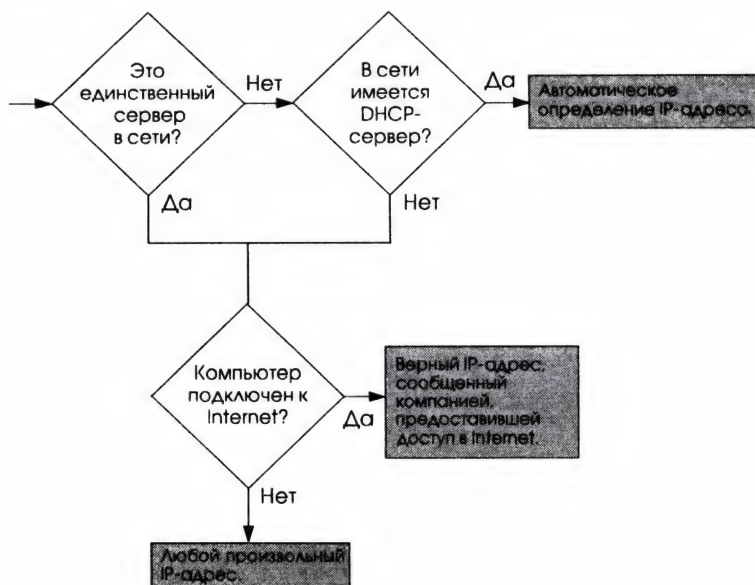
Если это не единственный сервер в сети, можно выбрать как фиксированный адрес, так и автоматически его получать от DHCP-сервера (при наличии такового, естественно). Что лучше? С точки зрения сервера, это в принципе не имеет значения. Вот, пожалуй, единственный минус использования DHCP-сервера для назначения адреса: если в момент обновления адреса на сервере Windows NT DHCP сервер будет недоступен (что маловероятно), адрес не будет назначен, и сервер потеряет связь с сетью по протоколу TCP/IP.

Если устанавливаемый сервер будет выполнять роль DHCP-сервера, то он однозначно должен иметь фиксированный адрес. Если при этом данный компьютер используется для связи с Internet, установите на нем DNS Server, взяв его либо из Windows NT resource Kit, либо у сторонних фирм.

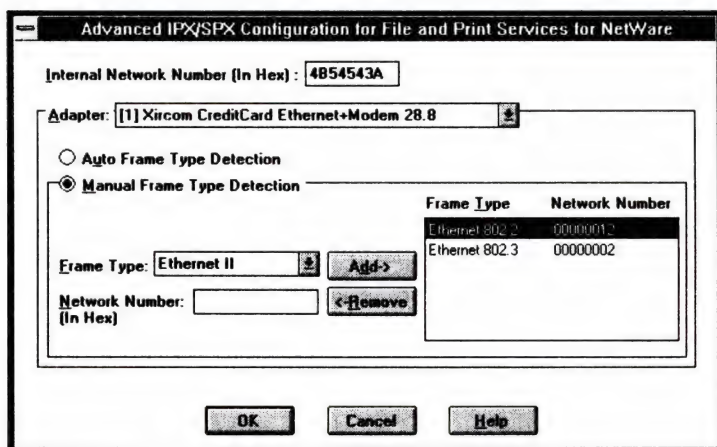


DNS-сервер включен в поставку Windows NT Server 4.0.

Схематично алгоритм выбора конфигурации TCP/IP показан на следующем рисунке.

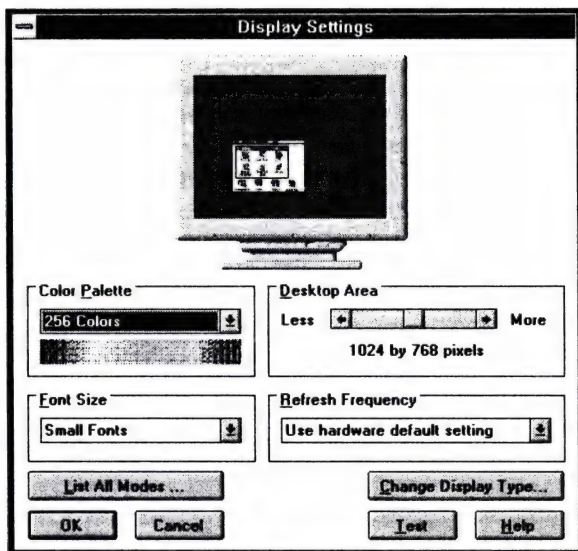


Для протокола IPX/SPX потребуется указать такой параметр, как Frame type и номер сети. По умолчанию устанавливается некоторый произвольный номер и автоматическое определение типа фрейма. Обычно этого достаточно, однако если Вы планируете работать совместно с серверами Netware, укажите точный номер сети и тип (типы) используемых фреймов.



Диалоговое окно конфигурации протокола IPX/SPX.

4. Программа установки попытается автоматически определить тип **видеоадаптера**, предложив Вам результат для утверждения. Не спешите "нажимать" ОК — выберите желаемое разрешение экрана, количество цветов, частоту развертки и щелкните кнопку **Test**.



Диалоговое окно Display Settings.

Тестовое изображение пробудет на экране 5 секунд. Внимательно рассмотрите его. Опыт показывает, что порой минимальные искажения тестовой картинки обернутся в дальнейшем невозможностью работы.

Если картинка просто не видна, значит, либо видеоадаптер, либо монитор не поддерживает установленный режим.

Если нарушена частота строк, выберите другое значение частоты.

Если некоторые буквы искажены или заменены на произвольные символы, будьте внимательны — это свидетельствует о том, что универсальный видеодрайвер несовместим с используемым видеоадаптером. Попробуйте либо указать иное количество цветов, либо выберите драйвер, поставляемый производителем. При отсутствии такого драйвера выберите стандартный режим VGA. В качестве примера рассмотрим компьютер DELL, в котором на материнской плате установлен видеоадаптер, базирующийся на микросхеме S3 764. Программа установки правильно определит тип кристалла — S3 и предложит установить для него режим 256 цветов при разрешении 640 x 480 точек. Однако при просмотре тестового изображения обнаружится, что буквы произвольно изменяют свой размер. Выбрав

16 или 65 535 цветов, Вам удастся избежать этих искажений. Потом на сервере www.s3.com можно найти видеодрайвер для используемого типа кристалла и установить его вместо стандартного.

Установка Windows NT на большое число компьютеров

Если в Вашей организации много компьютеров, Вы наверняка не раз задавались вопросом, как бы побыстрее установить на них операционную систему типа Windows NT, как "растиражировать" ее по всему предприятию. Если компьютеры однотипные, задача весьма проста.

Но сначала определимся с термином "однотипные компьютеры". К таким относятся машины, имеющие примерно одинаковый тип материнской платы и одинаковый набор дополнительных устройств. Критичным в данном случае являются фирма-изготовитель, тип адаптера жесткого диска и тип проигрывателя CD-ROM. Рассмотрим несколько примеров.

Если Вы установили систему на компьютер фирмы Compaq и использовали систему, записанную на Compaq SmartStart, не пытайтесь перенести эту систему на компьютер Hewlett-Packard. Если же система стоит в компьютере, имеющем SCSI-диски, перенос на машину с IDE-дисками также не доставит Вам удовольствия. Но если в оригинальном компьютере установлен видеоадаптер Cirrus Logic, а в компьютере, на который надо перенести систему, иной VGA-совместимый адаптер, все пройдет без сучка, без задоринки.

Как же выполнять перенос системы? Рассмотрим идеальный случай: Вы переносите систему на точно такой же компьютер, отличающийся, может быть, только объемом оперативной памяти или количеством жестких дисков.

Последовательность переноса такова.

- Скопируйте с исходного компьютера каталог, содержащий систему, на любой диск компьютера-приемника. Копирование можно выполнять либо по сети, либо временно вынув диск из второго компьютера и подключив его к компьютеру-оригиналу.
- Скопируйте с диска C: файл BOOT.INI на диск C: приемника. Если Вы скопировали систему на диск, имеющий другую букву, внесите соответствующую правку аналогично тому, как это показано ниже.


```
[boot loader]
timeout=30
default= multi(0)disk(0)rdisk(0)partition(2)\WINNT35S
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINNT35S="Windows NT Server Version 3.51"
multi(0)disk(0)rdisk(0)partition(2)\WINNT35S="Windows NT Server Version 3.51
[VGA mode]" /basevideo /sos
C:\="MS-DOS"
```

- На компьютере-приемнике: если раздел, на котором будет диск C:, не является активным, активизируйте его с помощью стандартной программы **FDISK**.
- На компьютере-приемнике: вставьте загрузочную дискету программы установки Windows NT Server, начните с нее выполнение программы установки и выберите опцию **Repair**. В качестве параметров восстановления укажите только **BOOT files**.

Выполнив описанную последовательность действий, загрузите компьютер-приемник. На нем уже будет установлена система Windows NT. Первое, что надо будет сделать после загрузки системы, — изменить имя компьютера и (при наличии такового) его IP-адрес.

Если в компьютере-приемнике установлены дополнительные устройства или некоторые не используются, зайдите в **Control Panel** и добавьте поддержку новых и удалите ненужные.

В любом случае подобный перенос системы займет гораздо меньше времени, чем ее установка.



Кстати: Описанная выше процедура может пригодиться Вам и при замене жесткого диска. Это позволит обойтись без переустановки всех приложений.



- В Windows NT Server 4.0 программу установки можно выполнить без вмешательства со стороны человека. Все, что требуется, — это создать сценарий установки, в котором заранее прописать все необходимые параметры. Этот сценарий может использоваться как самой программой **Setup**, так и Microsoft Systems Management Server, что позволяет быстро разворачивать сеть на базе Windows NT в больших организациях.

Защита информации и система безопасности Windows NT

Роль компьютерных сетей в бизнесе растет с каждым днем. Сети позволяют совместно работать с ключевой информацией и ресурсами большому количеству пользователей в организациях самых разных размеров. Часто информация, хранимая на сетевых серверах вроде Microsoft® Windows NT™ Server, является секретной и предназначена для ограниченного круга лиц. Предотвращение несанкционированного доступа к такого рода информации — основа защищенности и конкурентоспособности организации.



Защищенная система — уровень C2 и лучше

Защищенная сетевая система характеризуется рядом параметров. Каждая страна вырабатывает свои критерии защиты. В США, например, базовым критерием защиты являются рекомендации Министерства обороны на соответствие уровню защиты C2. Поскольку большинство правительственных учреждений США ориентируется именно на этот уровень, можно считать, что C2 должен обеспечиваться и в других организациях, заботящихся о безопасности информации. Важнейшие требования уровня защиты C2 таковы:

- Владелец ресурса (например, файла) должен иметь возможность контроля доступа к ресурсу.
- Операционная система должна защищать находящиеся в памяти компьютера и принадлежащие одному процессу данные от случайного их использования другими процессами. Например, Windows NT Server защищает участок памяти, занятый процессом так, что его содержимое не может быть прочитано даже после того, как процесс освободил его. Кроме того, при удалении файла с диска пользователи не должны иметь доступа к его данным, даже если дисковое пространство, ранее занятое удаленным файлом, выделяется для использования новым файлом.
- Каждый пользователь должен быть уникальным образом идентифицирован в системе, а система — иметь возможность применения этой идентификации для отслеживания всей деятельности пользователя.
- Администраторы системы должны иметь возможность аудита всех событий, связанных с защитой системы, а также действий отдельных пользователей. Правами доступа к данным аудита должен обладать ограниченный круг администраторов.
- Система должна защищать себя от вмешательства вроде модификации работающей системы или файлов, хранящихся на диске.

Есть и дополнительные требования, предъявляемые самой жизнью, — они относятся к управлению и использованию защиты. Среди них:

- возможность контроля со стороны администратора за тем, какие и кем используются ресурсы;
- возможность централизованного управления привилегиями и правами;
- возможность включения пользователей в группы, установки допустимого времени работы и т. п.
- возможность аудита таких событий, как попытка регистрации, доступа к файлам, принтерам и т.д.;
- блокировка учетных записей при неверной регистрации;
- установление срока жизни и правил использования пароля.

Windows NT Server, разработанный в соответствии с требованиями уровня C2, предлагает ряд дополнительных средств как для управления, так и использования этих дополнительных требований.

Уровень защиты C2 — определение требований

Требования уровня защиты C2 определены в издании Национального центра защиты компьютеров (NCSC) Министерства обороны США — Trusted Computer System Evaluation Criteria, известном как “Оранжевая книга”. Независимо от того, являются они отдельно стоящими или сетевыми операционными системами, в США они оцениваются по критериям, установленным в Оранжевой книге. Windows NT Server изначально разрабатывался в соответствии с требованиями Оранжевой книги.

Microsoft и NCSC тесно сотрудничали в процессе разработки, чтобы добиться соответствия Windows NT Workstation и Windows NT Server правительственным требованиям, предъявляемым к системам уровня C2.

NCSC опубликовал также различные “интерпретации” Оранжевой книги, разъясняющие положения этого документа применительно к различным условиям работы и компонентам системы. Так, издание Trusted Network, или “Красная книга”, — это интерпретация Оранжевой книги относительно сетевых компонентов защищенной системы.

В Красной книге требования не изменяются; здесь просто указано, как должна работать сетевая система, чтобы соответствовать уровню C2 Оранжевой книги. Существует полный набор интерпретаций Оранжевой книги, опубликованных NCSC в помощь поставщикам систем. Голубая книга интерпретирует требования Оранжевой к компонентам подсистем и т.д.

Сертификация Windows NT на уровень C2

Процесс сертификации занимает немало времени. По окончании сертификации продукты заносятся в “Список продуктов, соответствующих уровню C2”, публикуемый NCSC. Фирма Microsoft впервые подписала соглашение с NCSC о рассмотрении Windows NT на соответствие уровню защиты C2 в начале 1992 года, а в середине 1995 года Windows NT Workstation и Windows NT Server были включены в этот список. К настоящему времени на соответствие уровню C2 для отдельных систем сертифицированы Windows NT Server и Windows NT Workstation версии 3.5 с установленным дополнительно сервисным пакетом номер 3 (Service Pack #3). Это значит, что организации, в ко-

торых соответствие системы уровню C2 является ключевым условием, могут рассматривать использование Windows NT Workstation и Windows NT Server.

В настоящее время продолжается процесс сертификации Windows NT на соответствие уровню C2 по Красной и Голубой книгам. В Европе Windows NT Workstation и Windows NT Server находятся на этапе сертификации на соответствие уровню F-C2, E3, предполагающем более высокую степень защиты в сравнении с C2. Сертификация позволит пользователям как США, так и Европы работать с официально сертифицированной системой.

Решение реальных проблем защиты

Соответствие уровню C2 чрезвычайно важно для разработки защищенной операционной системы, однако большое количество "реальных" проблем защиты в Оранжевой книге напрямую не описано. При разработке системы защиты в Windows NT Server фирма Microsoft шагнула гораздо дальше требований C2.

Набор полноценных инструментов Windows NT Server облегчает администраторам управление и поддержку системы защиты. Администратор, например, может контролировать круг пользователей, имеющих права доступа к сетевым ресурсам: файлам, каталогам, серверам, принтерам и приложениям. Правами, определяемыми для каждого ресурса, можно управлять централизованно.

Учетные записи пользователей также управляются централизованно. Простыми графическими инструментами администратор задает принадлежность к группам, допустимое время работы, срок жизни и другие параметры учетной записи. У него также есть возможность аудита всех событий, связанных с защитой доступа пользователей к файлам, каталогам, принтерам и иным ресурсам. Система способна блокировать учетную запись пользователя при определенном числе неудачных попыток регистрации. Администратор устанавливает срок жизни паролей, может принуждать пользователей к периодической смене паролей и вводу паролей, которые сложно вскрыть.

С точки зрения пользователя, Windows NT Server обладает полноценной и несложной в обращении системой защиты. Простая процедура регистрации обеспечивает доступ к соответствующим ресурсам. Для пользователя невидимы такие процессы, как шифрование пароля на системном уровне, подразумевающее отсутствие передачи пароля в открытом виде по сети. Шифрование препятствует обнаружению пароля при несанкционированном просмотре сетевых пакетов. Пользователь определяет права доступа к ресурсам, которыми он "владеет". Например, он может разрешить совместное использование своего документа, указав, кто и как именно может с ним работать. Разумеется, доступ к ресурсам предприятия контролируется только администраторами с соответствующими правами.

Пример более глубокой защиты в Windows NT Server — способность защищать данные, находящиеся в физической памяти компьютера. Система предоставляет доступ к таким данным только имеющим на это право программам. Если данные больше не содержатся на диске, Windows NT Server предотвращает несанкционированный доступ к той области диска, где они содержались, и никакая программа не “подсмострит” информации, с которой оперирует в данный момент другое приложение в физической памяти машины.

Обеспечение защиты в корпоративной системе

Построение защищенной сетевой операционной системы требует тщательного планирования. Функции защиты должны быть включены в систему повсеместно. Файловая система, каталог учетных записей пользователей, система аутентификации пользователей, подсистемы, управление памятью — все требует серьезной проработки и четкого планирования.

Однако стандарты защиты для некоторых условий еще не определены. Пример — защищенность удаленного доступа. Дозвон, сетевая маршрутизация, фильтрация сетевых протоколов или сервисов, сетевая регистрация и аутентификация, передача файлов, электронная почта, связь с Internet — вот неполный список областей, в которых проблемы защиты решает администратор систем. Применение разработок сторонних фирм нередко усугубляет эти проблемы: дополнительно встают вопросы совместимости, мощности и наращиваемости.

Поддержка системы безопасности корпорации

Основой защиты корпорации является структура безопасности: ее определение, реализация и управление.

Система контроля за безопасностью организации должна соответствовать риску, связанному с компонентами информационных технологий. Она должна отражать структуру бизнеса и информационные потоки. Весь персонал должен знать процедуры и правила защиты информационных ресурсов и поддерживать высокую степень целостности системы.

Администраторы системы обязаны сдать экзамены по Windows NT Server и Windows NT Workstation на звание Microsoft Certified Professional. Только тогда они смогут самостоятельно выполнять установку, обслуживание и организацию надежной сети. К тому же администраторы должны нести ответственность за конфигурирование системы, регулярное резервное копирование, ввод новых пользователей и создание групп, использование ресурсов.

Вся информация, необходимая для грамотного администрирования, содержится в следующих изданиях:

- Документация на Microsoft Windows NT Server и Windows NT Workstation;
- *Windows NT Resource Kit, version 3.51* — пятитомное издание Microsoft Press;
- *Windows NT 3.5 Guidelines for Security, Audit, and Control* (Microsoft Press).

Модель безопасности Windows NT

В отличие от большинства операционных систем — вроде Windows, MS-DOS или OS/2 — Windows NT сконструирована так, что средства защиты встроены изначально в саму систему как часть спецификаций на разработку. Прежде чем получить доступ к любому ресурсу, пользователь обязан зарегистрироваться независимо от того, где он работает — на Windows NT Server или Windows NT Workstation. Windows NT обеспечивает защиту на локальном уровне, так как каждый компьютер имеет свою локальную базу политики защиты. Компоненты модели защиты осуществляют контроль за тем, кому и к каким объектам (например, файлам или принтерам) предоставляется доступ, какие действия разрешено производить и какие необходимо занести в журнал.



Кстати: Хотя многие аспекты безопасности являются общими для Windows NT Workstation и Windows NT Server, здесь мы рассматриваем в основном особенности Windows NT Server. Централизованная модель администрирования доменов Windows NT Server предпочтительнее при создании систем клиент-сервер. Применение одноранговых свойств Windows NT Workstation не рекомендуется, так как с ростом числа компьютеров управление такой системой резко усложняется.

Подчеркнем: система безопасности — это интегральная часть Windows NT, а не некоторая среда, причем действие ее распространяется на всю операционную систему.

Ключевыми элементами подсистемы защиты являются:

- Распорядитель локальной безопасности (Local Security Authority — LSA);
- Менеджер защиты учетных записей (Security Account Manager — SAM);
- Справочный монитор защиты (Security Reference Monitor — SRM).

Кроме того, в Windows NT имеются следующие элементы защиты:

- процесс регистрации;
- элементы управления персональным доступом;

- маркеры доступа;
- списки контроля доступа (Access Control List — ACL).

Эти элементы составляют основу защиты в Windows NT. Ниже рассматриваются компоненты подсистемы защиты, их взаимодействие и интеграция в систему.

Распорядитель локальной безопасности

Подсистема *Распорядитель локальной безопасности* (Local Security Authority — LSA) — сердце защиты в Windows NT Server. В его обязанности входит:

- предоставление пользователям доступа в систему;
- создание маркеров доступа в процессе регистрации;
- управление интерактивным процессом аутентификации пользователя
- разрешение Windows NT Server подключаться к программам аутентификации третьих фирм;
- управление локальной политикой защиты;
- контроль политики аудита;
- запись сообщений аудита, посылаемых Справочным монитором защиты, в журнал событий.

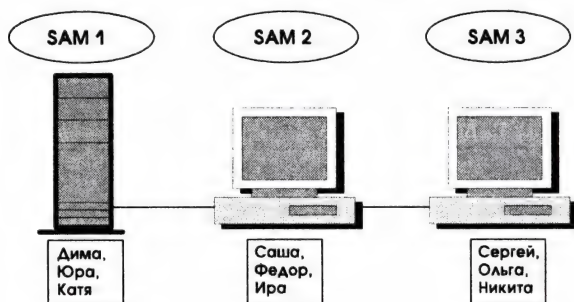
Менеджер защиты учетных записей

Менеджер защиты учетных записей (Security Account Manager — SAM) обслуживает работу с базой данных защиты учетных записей, известной как база SAM, в которой содержится информация обо всех учетных записях пользователей, групп и компьютеров. SAM обеспечивает сервис проверки пользователей, применяемый LSA. Невидимый для пользователя Менеджер защиты учетных записей отвечает за сравнение информации, вводимой пользователем в диалоговом окне **Welcome**, с той, что хранится в базе защиты, а также за предоставление пользователю его идентификационного кода (SID), а также SID всех групп, членом которых он является.

Удаление пользователя уничтожает его SID. Удаленная учетная запись пользователя не восстанавливается, так как для него больше не существует SID. Новая учетная запись с тем же самым именем получит новый SID, и, следовательно, у него не будет привилегий, имевшихся у предыдущей учетной записи.

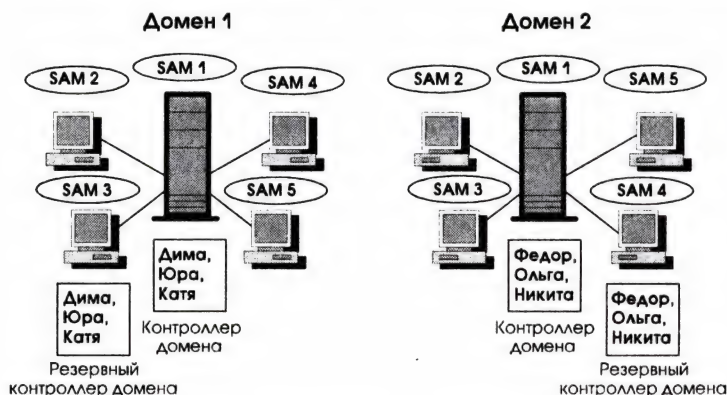
В зависимости от конфигурации сети могут существовать различные базы SAM на одной или нескольких системах с Windows NT. Выбор конкретной базы SAM определяется тем, где именно пользователь регистрируется — на рабочей станции или в сети. Например:

- В сети, где пользователи имеют локальные учетные записи на каждой рабочей станции, осуществляется доступ к базе SAM, расположенной на том компьютере, где регистрируется пользователь.



База SAM при использовании отдельных учетных записей на рабочих станциях.

- В сети с централизованной базой учетных записей пользователей [например, в однодоменной сети (о доменах см. раздел *Доменная структура сети и взаимоотношения доменов*)] имеется одна база SAM, расположенная на контроллере домена. При попытке зарегистрироваться на рабочей станции используется база SAM рабочей станции, а при попытке зарегистрироваться в домене — база SAM домена.
- В сети с централизованной базой учетных записей (например, в сети с одним мастер-доменом) имеется центральная база SAM, расположенная на первичном контроллере домена. Эта база тиражируется на резервные контроллеры домена. При попытке зарегистрироваться на рабочей станции используется база SAM рабочей станции, а при попытке зарегистрироваться в домене — база SAM первичного контроллера домена или одного из резервных контроллеров. Резервные контроллеры помогают разгрузить первичный контроллер. Windows NT Server, сконфигурированный как сервер, не участвует в процессе аутентификации пользователя.

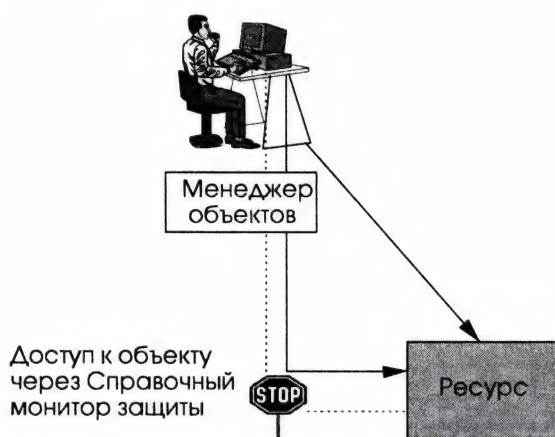


База SAM в сети с одним мастер-доменом.

Справочный монитор безопасности

Справочный монитор безопасности (Security Reference Monitor — SRM) — компонент Windows NT, предназначенный для усиления политики авторизации доступа и политики аудита, проводимых подсистемой Распорядителя локальной безопасности. Он обеспечивает защиту ресурсов или объектов от неавторизованного доступа или модификации. SRM предоставляет услуги для авторизации доступа к объектам, проверки субъектов (учетных записей пользователей) на привилегии и вывод необходимых сообщений аудита. Справочный монитор безопасности содержит только копию кода проверки доступа в систему, что гарантирует осуществление однотипной защиты объектов в Windows NT независимо от типа объекта.

Прямой доступ к объектам в Windows NT не разрешен: все запросы пользователей на доступ к объекту сначала проверяются Справочным монитором безопасности. Например, когда файл открывается на редактирование, Windows NT сравнивает дескриптор защиты файла с информацией о защите, хранящейся в маркере пользователя, и делает вывод о возможности предоставления доступа к файлу. Дескриптор защиты включает в себя все входы контроля доступа (ACE), создающие список контроля доступа (ACL) к файлу. Файл, у которого отсутствует ACL, открыт любому пользователю для любого вида доступа. Справочный монитор безопасности проверяет все ACE в ACL, определяя для конкретного пользователя возможность выполнить определенный вид доступа. Если SRM выдал разрешение на доступ к файлу, дополнительные проверки не ведутся. Дальнейшие попытки доступа к этому файлу осуществляются через созданную ссылку на этот файл.



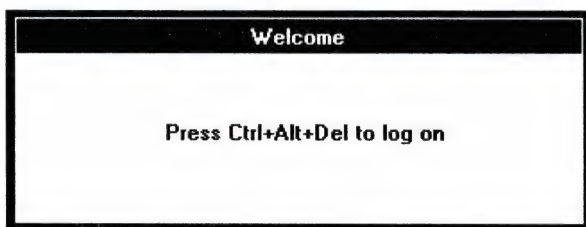
Допустим, Катя обладает доступом типа Print к объекту LaserPrinter. На то, чтобы напечатать документ “Мое выступление”, у нее есть 5 минут. Когда Катя сделает запрос к LaserPrinter на печать своего документа, Справочный монитор безопасности проверит через дескриптор защиты LaserPrinter, имеет ли Катин процесс (печать “Мое выступление”) права на LaserPrinter. Так как Катя этими правами обладает, она сможет распечатать свой документ.

Прошла минута, а распечатки все нет. Открыв Print Manager, Катя видит, что в очереди на печать перед ее документом еще 20! Текст выступления надо представить через 4 минуты, и она решает изменить очередность печати и передвинуть свой документ на первое место. Увы, попытка обречена: ведь соответствующих привилегий у бедняжки нет.

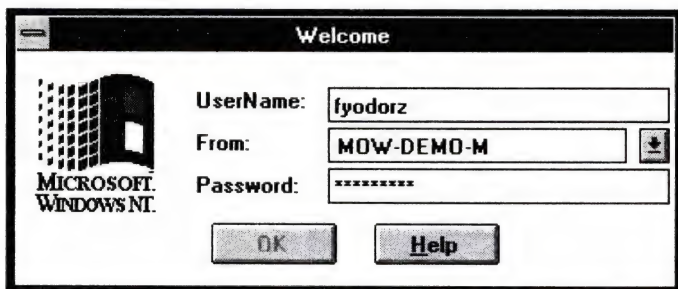
Справочный монитор безопасности невидим для пользователей, работает только с копией кода проверки доступа в систему и может защищать все объекты. SRM также генерирует сообщения, которые заносятся в журнал Распорядителем локальной безопасности.

Процесс регистрации

Интерактивный процесс регистрации — первая линия обороны Windows NT Server от несанкционированного доступа. Процесс начинается с диалогового окна, приглашающего нажать комбинацию клавиш Ctrl+Alt+Del. (Перед этим диалоговым окном может появиться предупреждение о легальности использования.) Такое начало процесса регистрации надежно защищает от любых программ, выполняемых в фоновом режиме, целью которых является выяснение регистрационных данных пользователя.



После этого появляется второе диалоговое окно процесса **WinLogon**.



Вводное диалоговое окно.

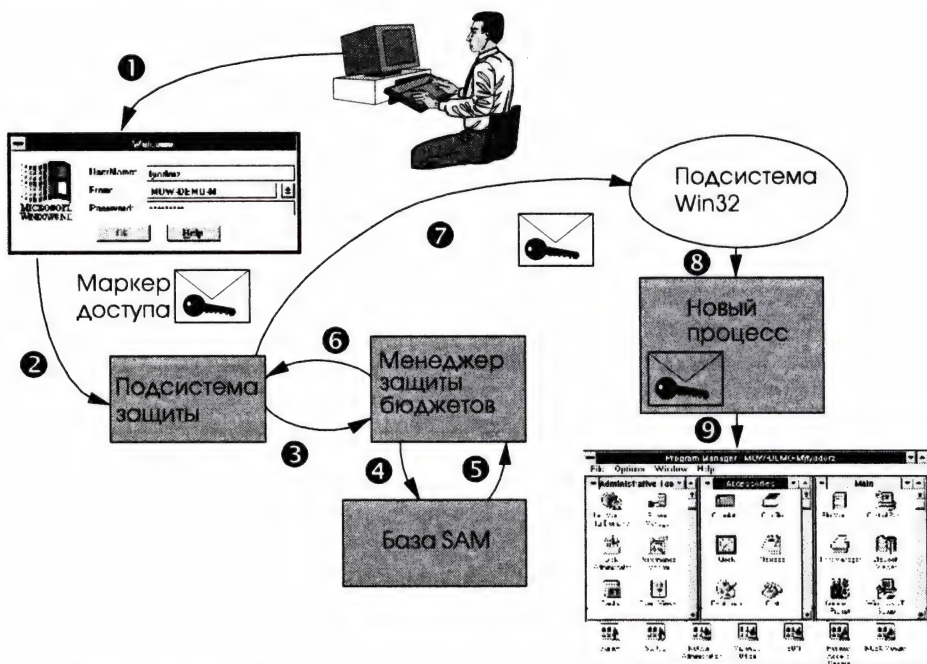
В этом окне пользователь вводит свое имя, имя сервера, рабочей станции или домена, в который ему необходимо получить доступ, и пароль. Если имя или пароль введены с ошибкой, система сообщит о невозможности авторизации доступа. При этом не сообщается, что именно — пароль или имя — вызвало ошибку. В случае правильного ввода имени, пароля и имени домена система переходит ко второму этапу — аутентификации пользователя.

Система аутентифицирует пользователя, передавая заданные в вводном диалоговом окне параметры в Менеджер защиты учетных записей (SAM). SAM сравнивает имя пользователя и пароль с хранящимися в базе пользователей домена. Если имя и пароль совпадают, сервер уведомляет рабочую станцию о подтверждении доступа. Сервер загружает и такую информацию, как привилегии учетной записи пользователя, положение домашнего каталога и т.п. Если для пользователя определен сценарий регистрации, он загружается на рабочую станцию для исполнения.

Если пользователь имеет учетную запись, его пароль верен и у него есть привилегии доступа в систему, подсистема защиты создает объект *маркер доступа*, представляющий пользователя. Он сравним с ключом, содержащим “удостоверение личности” пользователя. В нем хранится идентификатор защиты (SID), имя пользователя и имена групп, к которым он принадлежит.

Маркер доступа или его копия ассоциируются с любым процессом, выполняемым пользователем (например, открытие или печать файла). Комбинация процесс/маркер называется *субъектом*. Субъекты оперируют над объектами Windows NT, вызывая системные сервисы. Когда субъект осуществляет доступ к защищенному объекту, (например, файлу или каталогу), содержимое маркера сравнивается с содержимым списка контроля доступа к объекту (ACL), используя стандартную процедуру проверки. При этом определяется, можно ли субъекту предоставить право на выполнение запрашиваемой операции. Эта же процедура может при необходимости сгенерировать сообщения аудита, отражающие результат попытки доступа.

Созданный маркер передается процессу Win32 WinLogon. WinLogon предписывает подсистеме Win32 создать процесс для пользователя, и маркер доступа присоединяется к этому процессу. После этого подсистема Win32 инициирует Program Manager, который появляется на экране. На следующем рисунке изображен этот процесс.



Процесс регистрации.

Предупреждение о легальности использования

Это предупреждение, появляющееся после ввода комбинации Ctrl+Alt+Del в первом диалоговом окне **Welcome**, напоминает пользователю об ответственности, связанной с попыткой нелегального доступа в систему. Увидев его, пользователь должен щелкнуть кнопку ОК, чтобы подтвердить свои намерения. По умолчанию данное сообщение не выводится. Пользователь сам определяет заголовок окна и текст сообщения. Например, это может быть окно "Предупреждение пользователя!" с текстом "Система имеет ограничения на доступ. Только сотрудники фирмы имеют право доступа. Посторонним доступ воспрещен".

Для ввода этого текста используется редактор реестра (подробнее см. главу *Использование реестра*) и следующий ключ:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT
\CurrentVersion\Winlogon
```

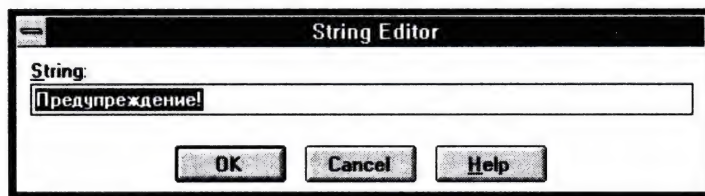
Чтобы изменить заголовок окна, дважды щелкните вход:

LegalNoticeCaption: REG_SZ

Чтобы изменить текст сообщения, дважды щелкните вход:

LegalNoticeText: REG_SZ

В появившемся диалоговом окне редактора строк введите желаемое сообщение или заголовок.



Диалоговое окно String Editor.

Регистрация в Windows NT 4.0

4.0

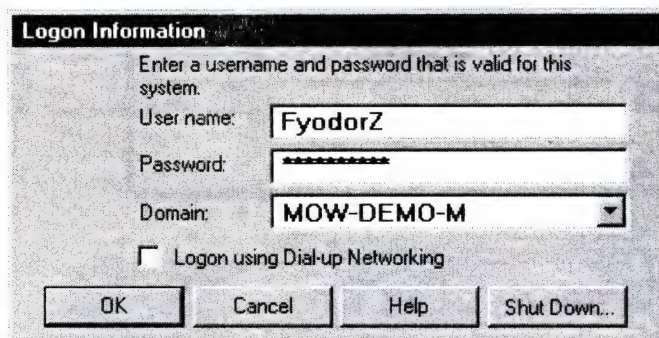
Важное дополнение внесено в процесс регистрации в Windows NT 4.0. Оно связано с возможностью осуществления регистрации в домене с помощью средств удаленного доступа к сети (о средствах удаленного доступа подробнее см. главу *Построение глобальных сетей и работа с Internet*).

Допустим, Вы часто работаете дома или не вылезаете из командировок, и система Windows NT Workstation установлена на Вашем ноутбуке или домашнем компьютере. Пока Вы работаете автономно, Вы не испытываете абсолютно никаких неудобств — зарегистрировавшись в системе локально, Вы имеете абсолютно прозрачный доступ к ресурсам компьютера. Картина радикально меняется при доступе к удаленным ресурсам (например, файлам на сервере в Вашей организации) с использованием RAS. Ведь в этом случае, с точки зрения контроллера домена, Вы оказываетесь “чужаком”. В базе SAM отсутствует Ваша “домашняя” учетная запись, и несмотря на то, что, регистрируясь при удаленном доступе, Вы указали имя, существующее в домене, Вам придется дополнительно указывать пароль, обращаясь к ресурсам домена.

Все было бы проще, имей Вы возможность, находясь вдали от родной конторы, зарегистрироваться в том домене, в котором Вы “живете” на работе. Вообще это возможно. Главным условием является хотя бы однократная предварительная регистрация компьютера в домене. В дальнейшем Вы будете аутентифицированы на основе информации, хранящейся в кэше, правда, при этом Вам не удастся внести изменения в базу SAM. Хорошо, если у Вас небольшой ноутбук: принесли на работу, подключились к локальной сети и разок зарегистрировались в домене. А если это домашний компьютер? Не нести же ради этого его на предприятие! Да и не факт, что Вас потом выпустят с ним назад.

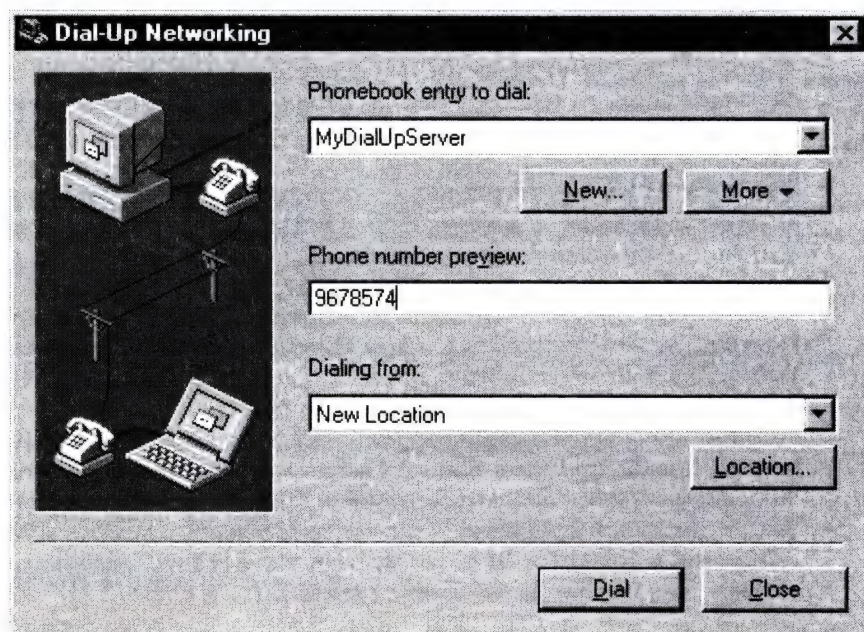
Вот тут на помощь и придет новая возможность — регистрация путем удаленного доступа к домену. С точки зрения пользователя, мало что изменяется. Все, что необходимо сделать при входе в систему, — указать

не только имя, пароль и имя домена, но и отметить флажок Logon using Dial-up Networking.



Диалоговое окно LogOn Information.

Вслед за этим выводится сообщение о запуске сервиса удаленного доступа (Dial-up Service), а потом появляется стандартное диалоговое окно **Dial-Up Networking**. Если Вы уже пользовались удаленным доступом на этом компьютере, достаточно выбрать соответствующую запись в телефонной книжке (Phonebook entry) и, при необходимости, место, откуда Вы осуществляете звонок.



Если к Вашему компьютеру подключен модем, соединенный с телефонной линией, произойдет соединение с сервером удаленного доступа с последующей аутентификацией Вас в домене.

Кстати: После регистрации в домене связь не обрывается. Вы можете продолжить нормальную работу и осуществлять доступ к ресурсам удаленной сети.

Настройка параметров удаленного доступа для регистрации

Описанный выше процесс регистрации по каналам удаленного доступа предлагается по умолчанию и в некотором смысле открыт для нелегального пользователя. На виду оказываются не только номера телефона сервера удаленного доступа, но и имя учетной записи, используемой для удаленного доступа. Кроме того, появляется возможность неограниченно манипулировать настройками и подбирать пароль входа в удаленную систему. Чтобы этого не случилось, настройте соответствующим образом параметры удаленной регистрации.

Для этого, вызвав программу **Dial-Up Networking**, щелкните кнопку **More**, затем в меню выберите команду **Logon Preferences**. В появившемся одноименном диалоговом окне имеется четыре раздела: **Dialing**, **Callback**, **Appearance**, **Phonebook**.

Замечание: Доступ к этому диалоговому окну открыт только пользователям, входящим в группу **Administrators**.

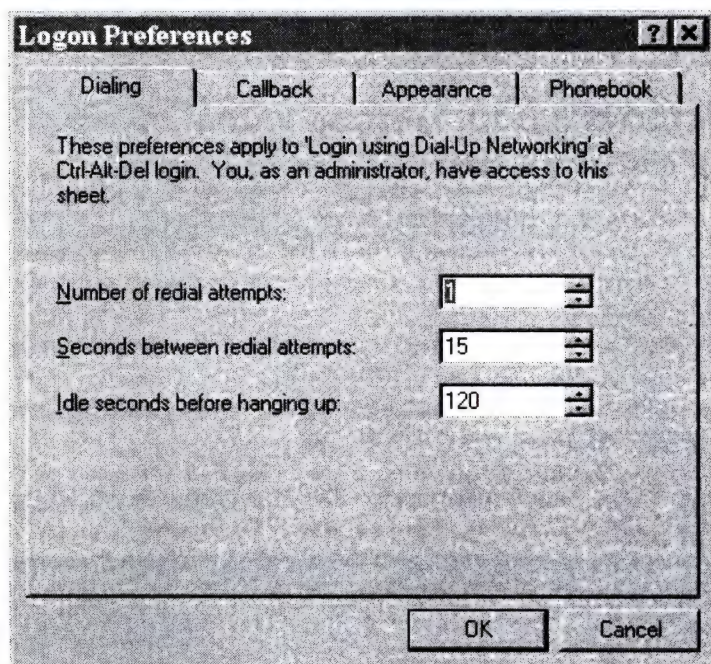
Параметры дозвона — Dialing

К основным параметрам дозвона относятся:

- **Number of Redial Attempts** (Число повторных звонков). Указывается, сколько раз можно повторить дозвон в случае неудачи (например, занятой линии). Для запрета повторных попыток укажите 0.
- **Seconds between redial attempts**. Интервал (в секундах) между первичным и повторным набором номера. Необходим для инициализации серверной стороны.
- **Idle seconds between hanging up** (Интервал бездействия). Если в течение этого промежутка времени со стороны пользователя не было никакой активности, удаленный доступ автоматически отключается от сервера.



Замечание: Аналогичный параметр имеется и на серверной стороне. Если Вы указали значение, превышающее установленное на сервере, будет использоваться интервал, указанный на серверной стороне.



Диалоговое окно Logon Preferences — Dialing.

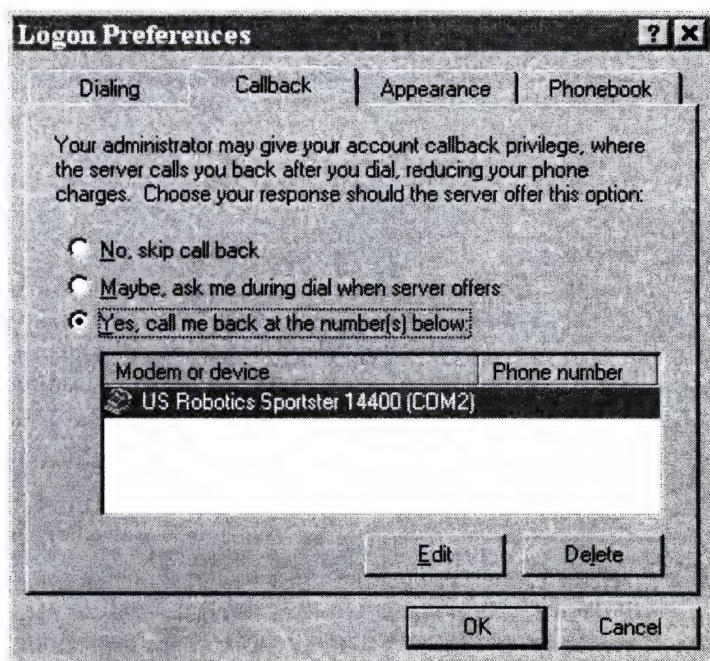
Параметры дозвона — Callback

Вторая группа параметров в значительной степени влияет на защищенность удаленной системы, так как позволяет регистрироваться в домене только пользователям, знающим определенный номер телефона. Для этого администратор системы может указать на сервере удаленного доступа на необходимость осуществления обратной связи (подробнее см. главу *Построение глобальных сетей и работа в Internet*).

На рабочей станции можно выбрать 3 вида реакции на запрос обратной связи:

- **No, skip call back** (Не использовать обратную связь). Предлагается по умолчанию. Возможности обратной связи не используются. Сделано исключительно для удобства пользователя, но в значительной степени снижает защищенность.

- **Maybe, ask me during dial when server offers** (Может быть, спросить по мере необходимости). Интерактивный режим в котором пользователю предлагается ввести номер телефона, по которому перезвонит сервер. Большое удобство для командированных. Это спасает их от нежелательных расходов, связанных с оплатой междугороднего телефонного звонка.
- **Yes, call me back at the number(s) below** (Да, перезвонить по телефонам, указанным ниже). Этот режим удобен для связи удаленного филиала с центральным офисом. Номера телефона (или телефонов) филиала меняются нечасто, что позволяет внести их в список, из которого сервер сможет выбрать один.



Диалоговое окно Logon Preferences — Callback.

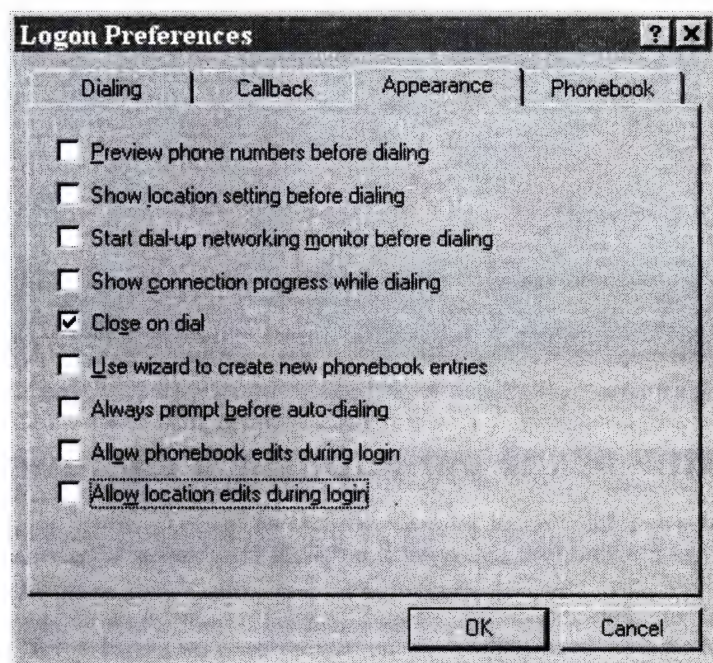
Параметры дозвона — Appearance

- Большая группа параметров, определяющих внешнее протекание процесса регистрации.
- **Preview phone numbers before dialing** (Просмотр номеров телефонов перед набором). Чтобы сохранить номер телефона сервера в секрете, не отмечайте этот флажок.

- **Show location setting before dialing** (Показ местоположения перед набором). По умолчанию система покажет название того места, откуда Вы осуществляете звонок. Для мобильных пользователей чрезвычайно удобный параметр, так как позволяет определить новое местоположение и тем самым — вид звонка (междугородний, международный или обычный).
- **Start dial-up networking monitor before dialing** (Запустить монитор удаленного доступа перед вызовом). По умолчанию этот флажок не отмечен, так как контроль за состоянием портов, количестве передаваемой информации и т.п. практически не нужен при регистрации в системе.
- **Show connection progress while dialing** (Показывать процесс соединения). Если отмечен этот флажок, пользователь видит протекание процесса регистрации удаленным сервером. Если это нежелательно, флажок отмечать не стоит.
- **Close on dial** (Закрыть после соединения). Диалоговое окно **Dial-Up Networking** будет закрыто сразу после успешного установления соединения.
- **Use Wizard to create new phone book entries** (Использовать программу-мастер для внесения новых номеров в книгу). Отметьте этот флажок, если на компьютере работает новичок, не способный самостоятельно определить параметры соединения. Специальная программа-мастер позволит ему сделать это быстро и безошибочно.
- **Always prompt before auto-dialing** (Всегда спрашивать о необходимости восстановления соединения). После регистрации пользователя в системе с удаленным доступом связь с удаленным сервером не прерывается. Канал используется для доступа к базе SAM. В случае прерывания связи и возникшей необходимости доступа к контроллеру домена Windows NT постарается автоматически восстановить связь с удаленным сервером. Если это нежелательно, отметьте флажок, и система будет запрашивать разрешение на восстановление связи. В противном случае восстановление будет выполняться "без спроса".
- **Allow phone book edits during login** (Разрешить редактирование телефонной книги при регистрации). Если к компьютеру могут иметь доступ неавторизованные пользователи, необходи-

мо запретить эту возможность, так как в противном случае Вы рискуете остаться без доступа к домену.

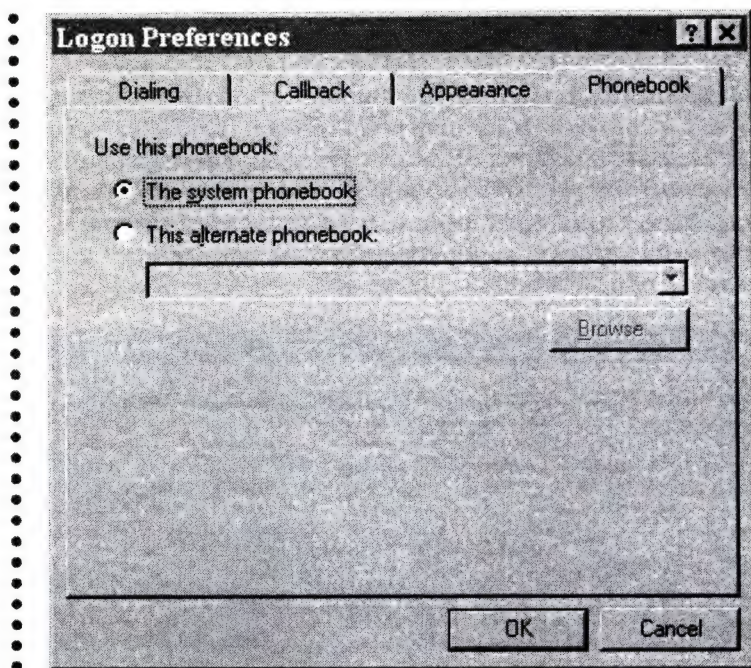
- **Allow location edits during logon** (Разрешить изменение параметра местоположения при регистрации). Как и в предыдущем случае, если к компьютеру могут иметь доступ неавторизованные пользователи, необходимо запретить эту возможность, поскольку в противном случае Вы рискуете остаться без доступа к домену или, самое лучшее, займетесь неблагодарной работой по восстановлению оригинальных значений.



Диалоговое окно Logon Preferences — Appearance.

Параметры дозвона — Phone book

- В последнюю группу параметров входят имена используемых телефонных книг. По умолчанию предлагается системная книга, хранящаяся в файле \SYSTEM32\rasphone.pbk. Если необходимый номер находится в другой книге, ее можно найти, “нажав” кнопку **Browse**.



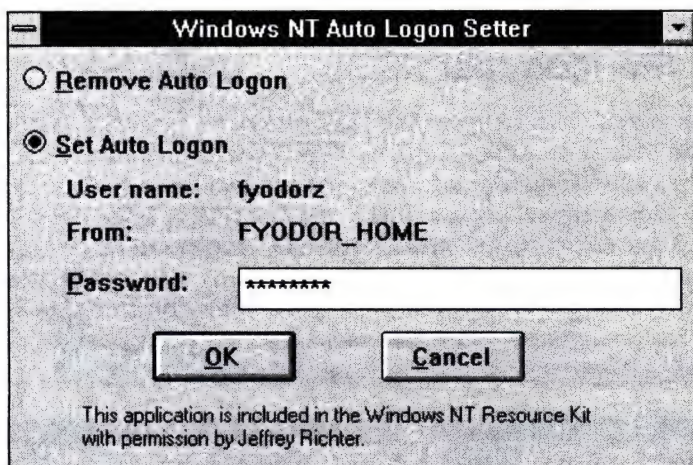
• Диалоговое окно Logon Preferences — Phonebook.

Автоматическая регистрация в системе

Если к защищенности Вашей системы не предъявляется никаких требований (например, система работает в автономном режиме и расположена в хорошо охраняемом помещении, или это Ваш домашний компьютер, за которым работает Ваш ребенок), можно разрешить автоматическую регистрацию в системе без ввода пароля. Тогда всякий раз при перезагрузке системы вместо диалогового окна с приглашением нажать Ctrl+Alt+Del будет выводиться Program Manager и будут запускаться все программы, расположенные в группе **Start-Up**.

При этом, разумеется, регистрация выполняется с использованием указанного Вами имени учетной записи. Права и привилегии, которыми обладает эта учетная запись, будут действовать в течение этого сеанса. Поэтому лучше создать специальную учетную запись, обладающую невысокими привилегиями и только для автоматической регистрации.

Чтобы переключиться на автоматическую регистрацию, лучше всего вызвать утилиту **Auto Logon** из Windows NT Resource Kit, хотя значения некоторых ключей в Реестре можно исправить и вручную. (Как это сделать, рассказано в Windows NT Resource Kit.)



Окно утилиты Auto Logon.

Элементы управления персональным доступом

Элементы управления персональным доступом позволяют владельцам ресурсов указывать, кто имеет права доступа к их ресурсам и как далеко этот доступ может простирается. Элементы контроля доступа, заданные в списках контроля доступа (ACL), определяют права доступа к ресурсам, предоставленные пользователям и группам. Системные ресурсы включают саму систему, файлы и каталоги, принтеры, ресурсы, совместно используемые в сети, и другие объекты.

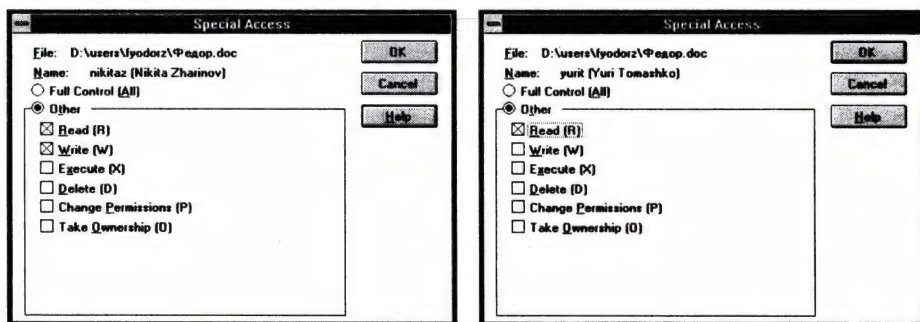
В таблице перечислены инструменты Windows NT, контролирующие доступ к ресурсам.

Инструмент	Позволяет
File Manager	Предоставлять файлы и каталоги в совместное использование в сети.
Print Manager	Предоставлять принтеры в совместное использование в сети.
User Manager for Domains	Управлять учетными записями пользователей и членством в группах; определять политикой безопасности.
Network (Control Panel)	Задавать пределы предоставления ресурсов для совместной работы другими пользователями сети.
Services (Control Panel)	Запускать и останавливать сетевые сервисы.

Рассмотрим несколько примеров, иллюстрирующих работу этих инструментов.

Определение персонального доступа к файлу с помощью File Manager

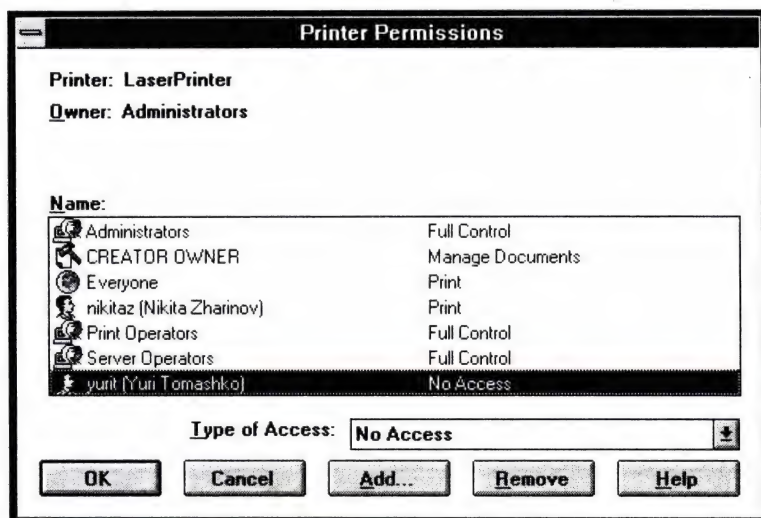
Допустим, пользователь fyodorz через File Manager предоставляет пользователю nikitaz доступ на чтение и запись к файлу Федор.doc, а пользователю yurit — только на чтение. При попытке yurit что-то записать в этот файл его запрос будет отвергнут. Другими видами доступа к файлам и каталогам являются: **No Access** (нет доступа), **List** (список), **Add** (добавить), **Add&Read** (добавить и чтение), **Change** (изменить), **Full Control** (полный доступ), **Execute** (исполнить), **Delete** (удалить), **Change Permissions** (изменить привилегии), **Take Ownership** (взять во владение). Ниже на рисунке показано, как устанавливать некоторые из них в **File Manager**.



Назначение специальных видов доступа в File Manager.

Определение персонального доступа к принтеру с помощью Print Manager

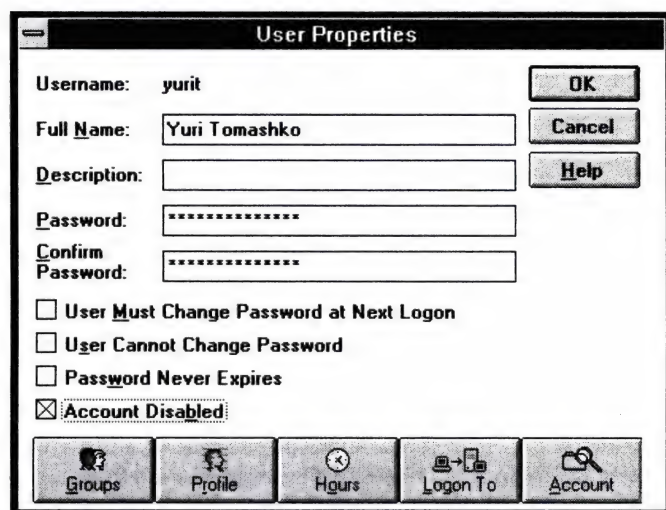
Администратор является владельцем принтера LaserPrinter. Он предоставляет пользователю nikitaz право **Print**, а пользователю yurit — **No Access**. Если yurit попытается послать документ на печать, его запрос будет отвергнут. Другими видами доступа являются **Manage Documents** (управление документами) и **Full Control** (полный контроль).



Назначение привилегий доступа к принтеру.

Определение персонального доступа для учетной записи пользователя с помощью User Manager for Domains

Будучи администратором Windows NT Server, fyodorz деактивизировал учетную запись yurit. Попытавшись зарегистрироваться в системе, yurit получит отказ.



Деактивизирование учетной записи пользователя.

Элементы управления персональным доступом можно применить для конкретных пользователей, нескольких пользователей, групп, ни для кого или для всех сразу, кто только может подключиться к сети Windows NT. Их могут устанавливать владельцы ресурсов, пользователи, имеющие доступ к учетной записи администратора, или любой пользователь, которому предоставлена возможность авторизации контроля доступа к ресурсам.

Маркеры доступа

Маркеры доступа являются объектами содержащими информацию о конкретных пользователях. Когда пользователь инициирует процесс, за этим процессом постоянно закрепляется маркер доступа.

Во время регистрации создание и применение маркера доступа критично. Когда пользователь или процесс пользователя пытается осуществить доступ к объекту, хранящиеся в маркере доступа SID и список групп, к которым принадлежит пользователь, сравниваются со списком контроля доступа ACL к объекту. Если в ACL есть разрешение на доступ пользователя или одной из групп, попытка закончится успешно.

Ниже в таблице перечислены самые общие объекты для маркеров доступа.

<i>Маркерный объект</i>	<i>Описание</i>
Идентификатор пользователя (SID)	Уникальным образом идентифицирует пользователя, для которого создан маркер.
Идентификатор группы	Идентифицирует группу(ы), к которой принадлежит пользователь.
Привилегии	Привилегии, назначенные пользователю.
Владелец	SID, назначаемый в качестве владельца любого объекта, созданного для пользователя, представленного данным маркером.
Первичная группа	SID, назначаемый в качестве первичной группы любого объекта, созданного для пользователя, представленного данным маркером. СПЕЦИФИЧНО ДЛЯ ПОДСИСТЕМЫ POSIX.
ACL по умолчанию	ACL, назначаемый по умолчанию любому объекту, созданному SID пользователя.

Списки контроля доступа

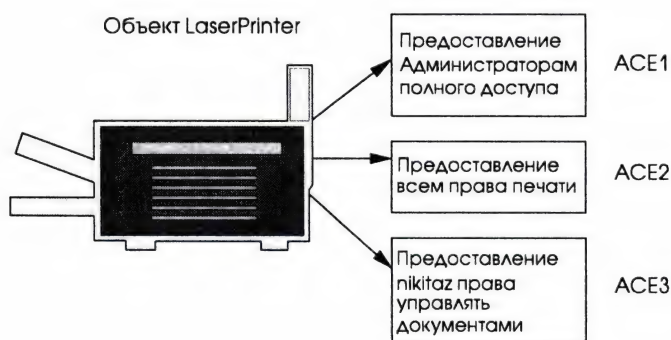
Списки контроля доступа (Access Control Lists — ACL) — форма персонального контроля доступа — работают совместно с файловой системой для защиты файлов от несанкционированного доступа. Каждый ACL состоит из *входов контроля доступа* (Access Control Entries — ACE), определяющих доступ к объекту. ACE, содержащие идентификаторы защиты и особые привиле-

гии доступа, вставляются в ACL при назначении пользователем персонального доступа к объекту. Если владелец объекта не установил персонального доступа к объекту, создается ACL по умолчанию. В таблице показано, какие средства применяются для администрирования различных списков контроля доступа.

Ресурс	Источник ACL
Файлы	File Manager
Принтеры	Print Manager
Пользователи	User Manager (для рабочих станций) User Manager for Domains (для серверов)

Когда пользователь осуществляет доступ к объекту, его персональный SID или SID одной из групп, к которой он принадлежит, сравнивается со списком ACE, а запрашиваемая деятельность — с возможностями доступа, описанными в ACE. В случае совпадения пользователю предоставляется доступ.

Например, Федор, являясь владельцем принтера LaserPrinter, предоставил через **Print Manager** Диме доступ к LaserPrinter с привилегией **Print**. Дима посылает документ на печать на LaserPrinter. Сразу же выполняется сравнение SID Димы с SID, записанным в ACE. Так как в ACE содержится разрешение на печать, документ Димы будет напечатан.



ACE сортируются по типу доступа — предоставить или запретить. В Windows NT сначала идет проверка ACE с отказом в доступе, а затем — с предоставлением доступа. Отказ всегда преобладает над предоставлением доступа.

Если хотя бы одной из групп, к которым принадлежит пользователь, запрещен доступ, то независимо от того, имеет ли разрешение на доступ он или остальные группы, в доступе будет отказано. Так что если группе **Everyone** (Все) запрещен доступ к объекту, значит, для всех пользователей, включая владельца ресурса, доступ к объекту запрещен. Значит, объект теперь закрыт отныне и навсегда для всех и каждого?! Только без паники. Незабвенный агент 007 советовал никогда не говорить “никогда”: запрещение доступа не запрещает владельцу ресурса изменить вид доступа к объекту!

Администрирование учетных записей пользователей

Пользователи компьютерной системы — основной фактор риска. Стоит их предоставить самим себе, и система неминуемо погибнет. Задача администратора — “разделять и властвовать”, позволяя выполнять рискованные операции самым опытным, а критичную информацию показывать только тем, кто имеет на это право. В основе управления пользователями в Windows NT Server — формирование локальных и глобальных групп, а также грамотная политика ведения учетных записей.



Учетные записи пользователей

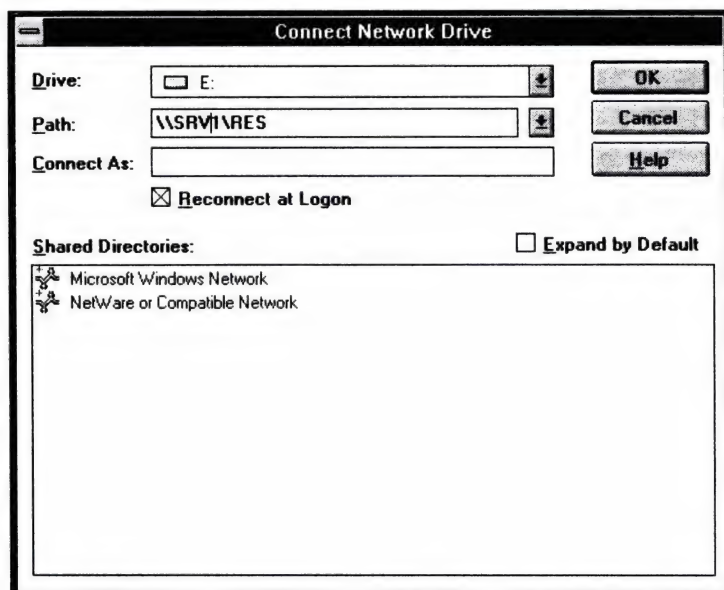
Любой пользователь Windows NT Workstation или Windows NT Server характеризуется наличием определенной *учетной записи*. Учетной записью называется совокупность прав и дополнительных параметров, ассоциированных с определенным пользователем. У каждого пользователя есть свое *имя* и *пароль*. В домене или в рабочей группе не может быть двух пользователей с одинаковым именем. В разных доменах имена могут совпадать, так как полное имя пользователя домена определяется по *совокупности Имя Домена\Имя Пользователя*. Скажем, если в доменах DOM1 и DOM2 есть пользователи с именем IVAN, в сети их полные имена различны: DOM1\IVAN и DOM2\IVAN.

При определении нового пользователя в системе формируется *идентификационный код* (*Security ID* — *SID*), по которому в дальнейшем система будет его распознавать. Этот уникальный код используется для доступа к ресурсам системы. **Именно этот код, а не имя пользователя определяет право на доступ к ресурсам.** Поэтому, если удалить какого-нибудь пользователя, а затем создать учетную запись для пользователя с таким же именем, что и у удаленного, "новичок" не получит доступа к ресурсам, доступным удаленному. Все дело в том, что идентификационный код "новичка" будет отличен от кода удаленного.

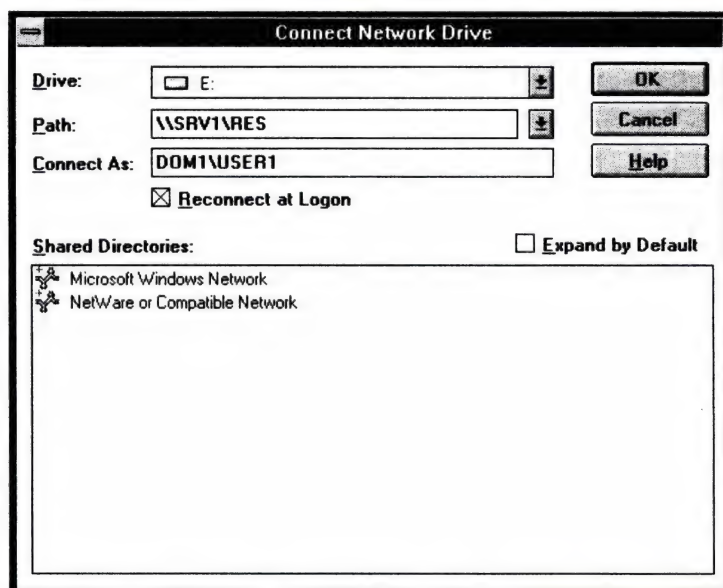
Локальные и глобальные учетные записи

Учетные записи пользователей Windows NT подразделяются на локальные и глобальные. Локальные учетные записи определяют права пользователей на конкретном компьютере и не распространяются на домен. Пользователь, зарегистрировавшийся в системе локально, получает доступ только к ресурсам этого компьютера. Если Windows NT Workstation принадлежит к рабочей группе, то локально зарегистрировавшийся пользователь с соответствующими правами получает доступ и к ресурсам невыделенных серверов этой рабочей группы. А чтобы обратиться к ресурсам домена, ему нужно каждый раз регистрироваться, используя свою глобальную учетную запись. Например, пользователь зарегистрировался на рабочей станции NTW1, входящей в домен DOM1, как *Administrator/NTW1*. Учетная запись Administrator является локальной для этой рабочей станции. Допустим, ему надо обратиться к файловому ресурсу RES, расположенному на сервере SRV1, также входящему в домен DOM1.

Тогда попытка подключения в Диспетчере файлов или с помощью команды NET USE * \\SRV1\RES приведет к отказу в доступе с выводом сообщения "*Access denied*". Для подключения к этому ресурсу используйте расширенный синтаксис команды NET: NET USE * \\SRV1\RES /USER:DOM1\USER1, где USER1 — глобальная учетная запись пользователя в домене DOM1. Или в поле **Connect as** Диспетчера файлов для доступа к ресурсу введите: DOM1\USER1.



Подключение к ресурсу домена, имеющего глобальную учетную запись для выбранного пользователя, при наличии доверительных отношений.



Подключение к ресурсу домена, имеющего глобальную учетную запись для выбранного пользователя, при отсутствии доверительных отношений.

Если пользователь осуществляет доступ к ресурсу, находящемуся в домене, с которым не установлены доверительные отношения и в котором нет для него глобальной учетной записи, то на сервере, содержащем необходимый ресурс, должна быть локальная учетная запись для пользователя.

Чтобы свободно обращаться к ресурсам домена, нужно зарегистрироваться в домене, используя свою глобальную учетную запись. Тогда аутентификация выполняется не на той рабочей станции, с которой пользователь вводит пароль и имя, а на главном или одном из резервных контроллеров домена.

Ниже в таблице показано, как назначать глобальные и локальные учетные записи для обеспечения разных уровней защищенности системы. При этом считается, что пользователь не входит в локальные или глобальные группы.

<i>Домен А</i>	<i>Домен Б</i>	<i>Доверительные Отношения</i>	<i>Степень защищенности</i>
○	×	×	Пользователь, локальная учетная запись которого на одном из серверов в домене А, имеет доступ только к ресурсам этого сервера. Доступ к ресурсам обоих доменов невозможен.
●	×	×	Пользователь, имеющий в домене А глобальную учетную запись, лишен доступа к ресурсам домена Б.
●	○	×	Пользователь, имеющий в домене А глобальную учетную запись, имеет локальную учетную запись на одном из серверов в домене Б и право доступа к ресурсам этого сервера. При этом требуется дополнительная регистрация пользователя на сервере.
●	●	×	Пользователь, имеющий в домене А глобальную учетную запись и глобальную учетную запись в домене Б, обладает правом доступа к ресурсам этого домена. При этом требуется дополнительная регистрация пользователя в домене.
●	×	Домен Б доверяет домену А	Пользователь, имеющий в домене А глобальную учетную запись, обладает правом доступа к ресурсам домена Б при условии, что домен А является доверяемым домену Б.

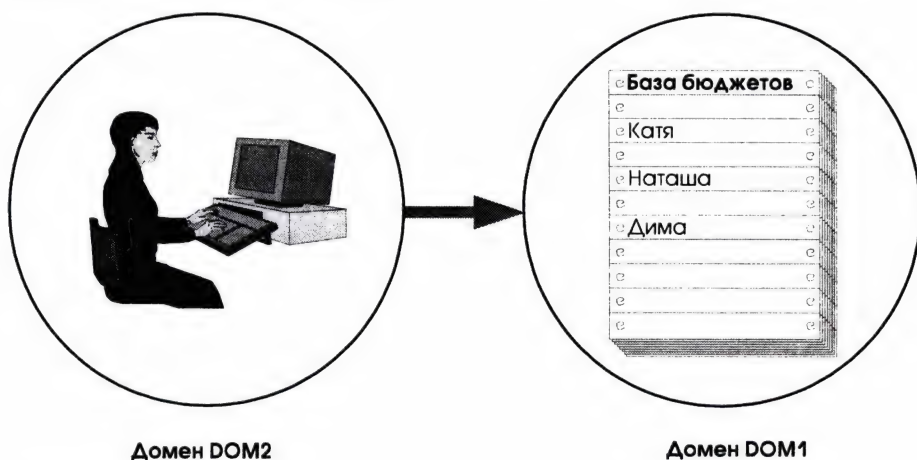
● — глобальная учетная запись; ○ — локальная учетная запись; × — отсутствие учетной записи

Сквозная авторизация

С помощью *сквозной авторизации* пользователь, имеющий учетную запись в одном домене, осуществляет доступ к ресурсам того домена, в котором у него учетной записи нет. Это обеспечивается доверительными отношениями между доменами. Сквозная авторизация происходит, когда локальный компьютер не может проверить пользователя, имеющего учетную запись в другом домене. В этом случае имя и пароль передаются на тот Windows NT Server, где пользователь может быть авторизован, а затем сведения о нем возвращаются на компьютер, с которого поступил запрос.

При сквозной авторизации пользователь может иметь учетную запись только в одном домене и все-таки обладать правом доступа ко всей сети. Например, Наташа — член домена DOM1. Она пришла в офис, все компьютеры которого входят в домен DOM2. DOM2 доверяет домену DOM1. Далее возможен такой сценарий:

1. Наташа пытается войти в систему, введя информацию о себе в диалоговом окне **Welcome**.
2. Так как она принадлежит домену DOM1, ее авторизация должна выполняться в домене DOM1.
3. Windows NT Server в домене DOM2 не может авторизовать ее.
4. Windows NT Server передает запрос на регистрацию в домен DOM1.
5. Windows NT Server в домене DOM1 регистрирует Наташу. Схематично этот процесс представлен на рисунке.



Сквозная авторизация.

Зарегистрировавшись, Наташа сразу получит доступ к ресурсам домена DOM1 и ресурсам, предоставленным в совместное использование в домене DOM2.

Сквозная регистрация имеет место в двух случаях:

1. При регистрации в доверяющем домене.
2. При доступе к ресурсам доверяемого домена.

Сквозная регистрация при доступе к ресурсам доверяемых доменов поддерживается всеми клиентами Microsoft Network. MS-DOS-клиенты (как LAN Manager 2.2 MS-DOS Enhanced, так и Workgroup Connection 2.x) не поддерживают сквозную регистрацию в доверяющем домене.

Создание и редактирование учетных записей пользователей

После установки Windows NT Workstation в системе будут две учетные записи: **Administrator** и та, что Вы создадите в процессе работы **Setup**. После установки Windows NT Server в системе также будут две локальных учетных записи: **Administrator** и **Guest**. Они называются встроенными. По умолчанию у **Administrator** очень большие возможности по управлению системой, а у **Guest** — предельно низкие. Но **Guest** может войти в систему без пароля. Это, несомненно, снижает уровень защищенности системы, поэтому лучше создайте новую учетную запись с административными правами, а учетные записи **Administrator** и **Guest** заблокируйте.

Для создания локальных и глобальных учетных записей служит **User Manager** из Windows NT Workstation. Эта программа позволяет создавать только локальные учетные записи для той рабочей станции, где она установлена. **User Manager**, находящаяся на одном из контроллеров домена, поможет создать локальные учетные записи для используемого сервера и глобальные учетные записи для того домена, на контроллере которого запущен **User Manager**, и для любого другого домена, доверяющего этому.

Создавая новую глобальную учетную запись или модифицируя уже имеющуюся, помните: если Вы запустили **User Manager** на одном из резервных контроллеров домена, главный контроллер должен быть доступен по сети. Дело в том, что модификация базы учетных записей возможна только на главном контроллере домена; резервные контроллеры хранят лишь копии этой базы, которые нельзя изменить.

Если в домене большое количество резервных контроллеров, для обновления базы учетных записей на всех контроллерах потребуется какое-то время, в течение которого только что введенный пользователь, возможно, не зарегистрируется в сети, так как его аутентификация будет выполняться тем контроллером, на котором база еще не обновлена. Чем меньше скорость канала между главным и резервным контроллерами, тем длительней этот период.

Создавая новую учетную запись Вы можете определить такие параметры:

- пароль;
- правила модификации пароля пользователем;
- локальные и глобальные группы, в которые входит пользователь;
- профиль пользователя;
- имена рабочих станций, с которых пользователь может регистрироваться в сети;
- разрешенные часы работы пользователя;
- срок действия учетной записи.

Ниже подробно описано назначение и применение каждого из этих параметров.

Пароль пользователя и правила его модификации

Вход в систему Windows NT обязательно сопровождается вводом пароля. Пароль и его параметры (минимальную длину, срок жизни и др.) назначает администратор системы, который также может определить, каким образом пользователь будет изменять пароль в будущем. После того как пользователь модифицирует пароль, администратор уже не сможет его узнать.

Чтобы добавить нового пользователя, выберите в меню программы **User Manager** команду **Add user**, а для модификации параметров уже имеющегося — дважды щелкните его имя в списке пользователей. После этого появится окно свойств пользователя.

Окно добавления нового пользователя в программе User Manager.

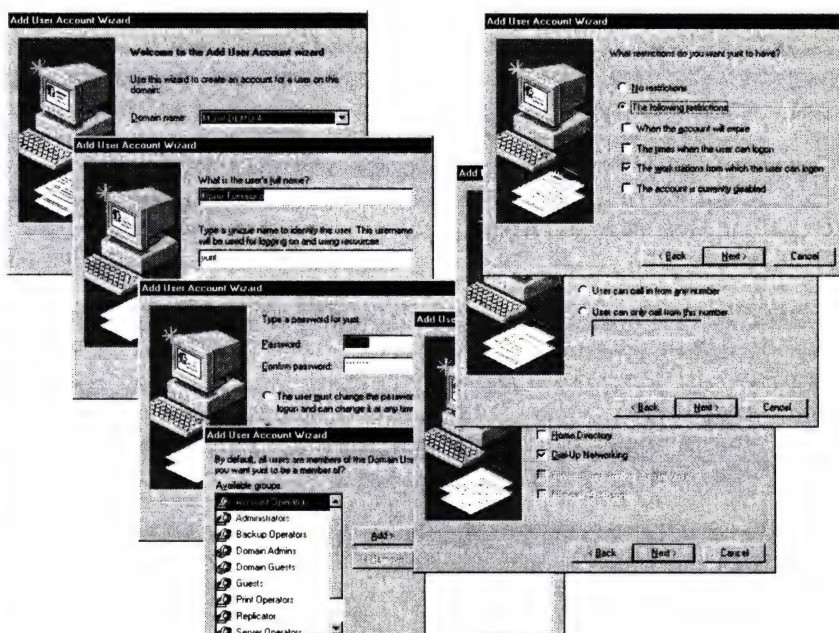
В этом окне администратор может пометить следующие флажки

Флажок	Действие
Users Must Change Password at Next Logon	Принуждает пользователя изменять пароль при первой регистрации в системе. Помечается по умолчанию при создании новых пользователей. Применяется администратором при создании новых учетных записей или назначении временных паролей.
User Cannot Change Password	Помечен по умолчанию для учетной записи Guest . Используется только для гостевых учетных записей, имеющих ограниченный доступ к ресурсам системы.
Password Never Expires	Имеет приоритет перед значением, заданным параметром Maximum Password Age в диалоговом окне, определяющем политику ведения учетных записей (см. раздел <i>Глобальные параметры, влияющие на защищенность системы</i>), и перед значением Users Must Change Password at Next Logon . По умолчанию не помечен. Настоятельно не рекомендую использовать: ведь постоянная смена паролей — одно из условий повышенной защищенности системы.
Account Disabled	Приостанавливает возможность применения учетной записи. Полезно устанавливать для учетных записей, которым временно надо запретить доступ, или для пользователей, которым долго не потребуется доступ (например, сотрудникам, находящимся в отпуске или длительной командировке).

Создание учетных записей пользователей с помощью программы-мастера

4.0

Для создания новой учетной записи с помощью *User Manager for Domains* следует знать о том, какие параметры прописывать обязательно, а какие нет. Начинаящий администратор может не обладать такими знаниями или просто забыть об определении тех или иных параметров. На помощь ему придет новая программа-мастер в Windows NT Server 4.0, позволяющая последовательно определять параметры учетной записи. Количество шагов в этой программе зависит от того, какие параметры выбираются и какие приложения установлены. Например, если Вы отметите в разделе ограничений, что данный пользователь должен иметь ограничение по рабочим станциям, с которых он имеет право регистрироваться в домене, то на следующем шаге программа-мастер попросит Вас ввести имена этих рабочих станций. На рисунке изображены некоторые диалоговые окна этой программы.



Шаги создания новой учетной записи в программе *Add User Account Wizard*.

- Инструмент настолько удобен, что даже опытный администратор с удовольствием воспользуется им — “текучка” может отвлечь его во время работы с **User Manager**, и тогда какое-либо ограничение не будет установлено для какого-нибудь сотрудника, а тот не упустит своего шанса. Программа-мастер, вероятно подобных упущений практически сводит к нулю (хотя не исключает преднамеренных действий).

Группы пользователей

Группой называется набор прав на доступ к ресурсам, присваиваемый сразу нескольким пользователям. С помощью групп удобно управлять доступом к ресурсам пользователей, выполняющих в Windows NT сходные задачи. Принадлежность к группе определяется в соответствии со служебными обязанностями пользователя, специальными требованиями к доступу или другими критериями.

Группы позволяют администратору рассматривать учетные записи большого числа пользователей как одну. При отсутствии групп сделать одинаковые изменения в учетных записях нескольких пользователей — труд неблагодарный и утомительный: Вам придется одну и ту же операцию выполнить столько раз, сколько учетных записей надо изменить. Если же эти учетные записи включены в группу, достаточно изменить учетную запись этой группы — и пользователи получат новые права.

Опытный администратор сети планирует группы как часть процесса установки сети. Новая учетная запись пользователя включается в различные группы при создании. При этом учитывайте, какие административные функции пользователь будет выполнять в сети и какой вид доступа к ресурсам ему необходим.

В зависимости от размера системы администратор должен решить, какие административные функции можно (или нужно) делегировать другим пользователям системы. Некоторые административные обязанности (например, резервное копирование и восстановление файлов, добавление в систему новых учетных записей пользователей, предоставление и прекращение совместного использования ресурсов) требуют наличия у пользователя определенных прав.

Для реализации многоярусной административной модели в Windows NT применяются три типа учетных записей:

- *Учетные записи пользователей.* У каждого пользователя в системе имеется своя защищенная паролем учетная запись. Учетные записи делятся на локальные и глобальные.
- *Локальные группы.* Локальные группы определяются на каждой машине. В них могут входить как учетные записи пользователей, так и глобальные группы. В Windows NT имеется ряд встроенных локальных групп.
- *Глобальные группы.* Глобальные группы определяются на уровне домена (что подразумевает наличие минимум одного Windows NT Server). В Windows NT встроен ряд глобальных групп.

Локальные группы

На отдельно стоящих Windows NT-системах создаются и поддерживаются только локальные группы. Локальная группа предоставляет права и доступ только для той системы, на которой она определена.

Если система является частью домена, в локальную группу могут входить учетные записи пользователей того домена, где находится локальная группа, или учетные записи доверяемых доменов.

Если в сети много доменов, локальные группы удобны для объединения нескольких глобальных групп в одно управляемое звено. Вместо присвоения прав каждой из глобальных групп администратор определяет права для одной локальной группы и включает в нее несколько глобальных. Членство в локальной группе домена позволяет пользователям других доменов иметь доступ к ресурсам этого.

В локальную группу могут входить:

- на уровне рабочей станции — учетные записи пользователей Windows NT Workstation. Не являются частью домена;
- на уровне домена — учетные записи пользователей домена, в котором определена локальная группа или учетные записи пользователей доверяемых доменов. Это справедливо, если машина входит в домен независимо от того, является она Windows NT Workstation или Windows NT Server;
- в любую — глобальные группы либо из того же самого домена, либо из доверяемых доменов.

На рисунке показано, как строятся локальные группы.

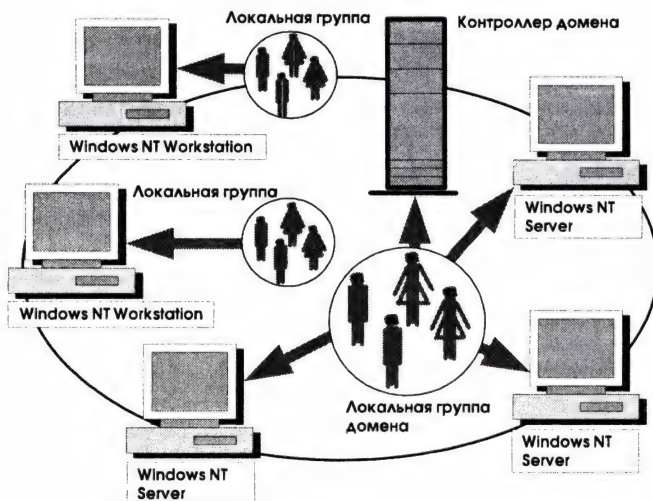
Правила локальных групп



Как видно, локальная группа может включать в себя учетные записи индивидуальных пользователей и глобальные группы, но не другие локальные группы. Например, локальная группа, созданная в домене DOM1, может:

- содержать учетные записи пользователей и глобальные группы этого домена и всех доверяемых доменов;
- использоваться только на серверах домена DOM1.

Существует два уровня локальных групп: *уровень рабочей станции* и *уровень домена*. Из названия понятно, что локальные группы первого уровня функционируют только на машинах с Windows NT Workstation, а второго — на машинах с Windows NT Server. На рисунке показано функционирование локальных групп на доменном уровне и уровне рабочих станций.



Локальные группы на рабочих станциях

Локальные группы работают только в той базе, где были созданы. Пользователь локальной группы на одной машине не имеет доступа к ресурсам другой машины. На Windows NT Workstation это ограничивает их этой рабочей станцией. Такие группы создаются с помощью **User Manager**. На Windows NT Server влияние групп распространяется на этот сервер и на те, куда база копируется (Windows NT Server-серверы в домене). Эти локальные группы создаются с помощью **User Manager for Domains**.

В локальные группы рабочих станций могут входить:

- учетные записи пользователей рабочей станции;
- учетные записи пользователей или глобальные группы домена, к которому принадлежит рабочая станция;
- учетные записи пользователей или глобальные группы доменов, доверяемых доменом, к которому принадлежит рабочая станция.

Локальные группы рабочей станции нельзя использовать на других рабочих станциях.

Локальные группы домена

Локальные группы домена могут использоваться только в домене и — более того — только в базах машин с Windows NT Server. Это значит, что пользователи локальных групп домена могут задействовать ресурсы только серверов с Windows NT Server, входящих в этот домен, но не ресурсы Windows NT Workstation или иных компьютеров. В локальную группу домена могут входить учетные записи пользователей локального домена или любого домена, доверяемого локальным. При этом доступ можно предоставить только к ресурсам того домена, в котором определена локальная группа.

Встроенные локальные группы

Как в Windows NT Workstation, так и в Windows NT Server встроено несколько локальных групп. В Windows NT Workstation встроены группы:

Administrators

Power Users

Users

Guests

Everyone

Backup Operators

Replicator

Windows NT Server включает те же группы (кроме **Power Users**) плюс:

Server Operators

Account Operators

Print Operators

О различиях между этими группами и присвоенных им правах см. раздел *Права пользователей и групп*.

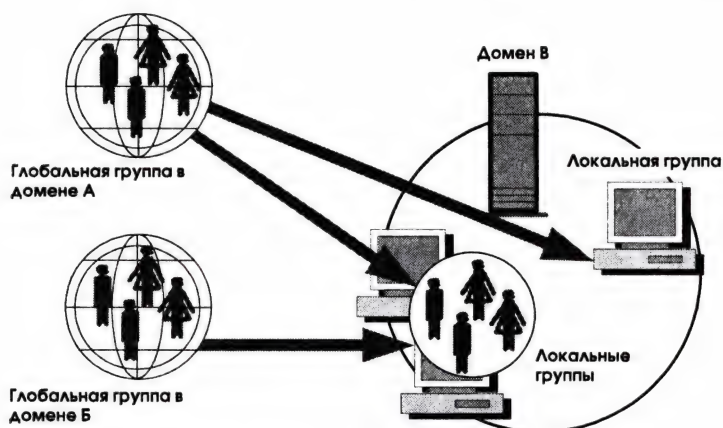
Глобальные группы

Глобальные группы — инструмент администратора домена, служащий для организации пользователей. Единственная цель глобальных групп — собрать пользователей вместе, чтобы поместить их в подходящую локальную группу. Глобальные группы не применяются для назначения административных функций или предоставления пользователям доступа к ресурсам.

Пользователям, входящим в глобальную группу, права назначаются путем включения глобальной группы в локальную с соответствующими правами. Это позволяет пользователям глобальной группы получить доступ к ресурсам на Windows NT Workstation или ресурсам локального или доверяемого домена.

Глобальная группа может включать учетные записи пользователей домена, но не другие глобальные группы.

На рисунке показано, как, включая глобальные группы из нескольких доменов в локальные, предоставляется доступ к различным ресурсам.



Обзор глобальных групп.

При создании учетная запись пользователя автоматически включается во встроенную группу **Domain Users**. Члены глобальной группы:

- должны быть учетными записями пользователей в том домене, в котором создана группа;
- могут использовать ресурсы любого домена, для которого глобальная группа имеет разрешение.

Через доверительные отношения между доменами учетные записи в глобальных группах могут получить доступ к ресурсам в любом месте сети независимо от того, где физически расположены эти ресурсы.

Глобальные группы не могут содержать ни локальных, ни глобальных групп. Члены глобальной группы — только учетные записи пользователей. Внутри собственного домена имена глобальных групп не включают префикса в виде имени домена. В других доменах имена глобальных групп содержат префикс. Например, глобальная группа **Domain Users**, созданная в домене DOM1, будет видна в домене DOM2 как **DOM1\Domain Users**.



Внимание: Имена глобальной и локальной групп могут совпадать.

Поскольку действие локальных групп распространяется только на те компьютеры, где тиражируется база учетных записей, глобальные группы в однодоменных сетях гарантируют равные возможности по доступу пользователей к ресурсам Windows NT Workstation и Windows NT Server при минимуме административных усилий.

Глобальные группы, встроенные в Windows NT Server

В Windows NT Server встроены три глобальные группы: **Domain Admins**, **Domain Users** и **Domain Guests**.

Domain Admins входит в локальную группу **Administrators** домена и в группу **Administrators** каждой рабочей станции Windows NT Workstation в домене. Чтобы предоставить новым пользователям административные полномочия, их включают в глобальную группу **Domain Admins**.

В группу **Domain Users** по умолчанию входят все пользователи домена, включая встроенные учетные записи пользователей и вновь создаваемые учетные записи.

Группа **Domain Guests** объединяет всех пользователей с правами гостя. По умолчанию в нее входит учетная запись **Guest**.

Стратегия использования групп

Определив задачи по управлению сетью, администратор должен решить, какие локальные группы способны выполнять те или иные задачи. Локальные группы, встроенные в Windows NT Server, охватывают практически все возможности по управлению сетью.

Если каждый домен представляет собой отдельное подразделение или отдел на предприятии, администратор может рассматривать глобальные группы как группы пользователей одного подразделения. Например, можно создать в каждом домене первого яруса глобальные группы высшего руководства каждого из подразделений. Тогда, чтобы предоставить высшему руководству доступа к финансовой информации в домене Финансового отдела, в нем создается локальная группа с соответствующими правами, включающую все глобальные группы высшего руководства из доменов первого яруса.

В другом домене такая глобальная группа пользователей может получить другие права и привилегии. Итак, глобальная группа — это средство экспорта нескольких пользователей как единого целого в другие домены и рабочие станции в сети. Если перед именем группы стоит имя домена, в котором она создана, администратор легко определит по имени группы ее права и по имени домена — место создания.

Ниже в таблице описаны иные способы использования групп:

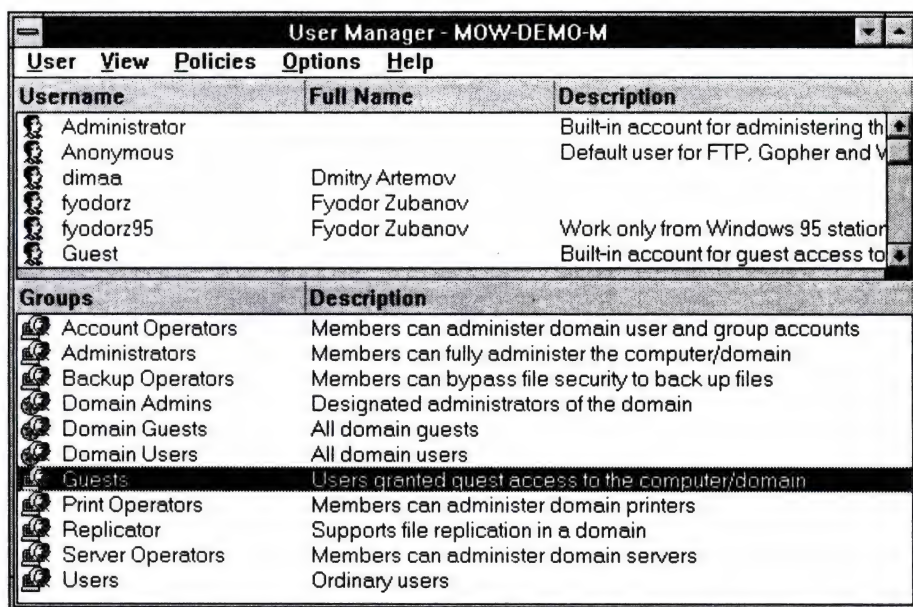
<i>Цель</i>	<i>Группа</i>	<i>Комментарий</i>
Сгруппировать пользователей домена в единое звено для применения в других доменах.	Глобальная	В других доменах глобальная группа может быть включена в локальные группы, или ей можно непосредственно присвоить определенные права.
Пользователям нужны права и привилегии только в одном домене.	Локальная	В локальную группу могут входить пользователи и глобальные группы из других доменов.
Пользователям требуются права на доступ к Windows NT Workstation.	Глобальная	Глобальные группы домена могут получить права на доступ к Windows NT Workstation, а локальные группы — нет.
Включать в себя другие группы.	Локальная	В локальную группу могут входить только глобальные группы (и пользователи). Однако другие локальные группы не могут входить ни в какую группу.
Включать в себя пользователей из других доменов.	Локальная	Локальная группа используется только в том домене, где была создана. Чтобы предоставить этой группе права в других доменах, она должна быть создана в каждом из этих доменов.

Создание и модификация групп

Локальные и глобальные группы создаются с помощью **User Manager** (для Windows NT Workstation) и **User Manager for Domains** (для Windows NT Server).

Группы управляются с помощью диалоговых окон **Group Properties** или **User Properties**. В **Group Properties** Вы работаете со списком пользователей, включенных в ту или иную группу. А в **User Properties** для каждого пользователя определяются группы, к которым он принадлежит.

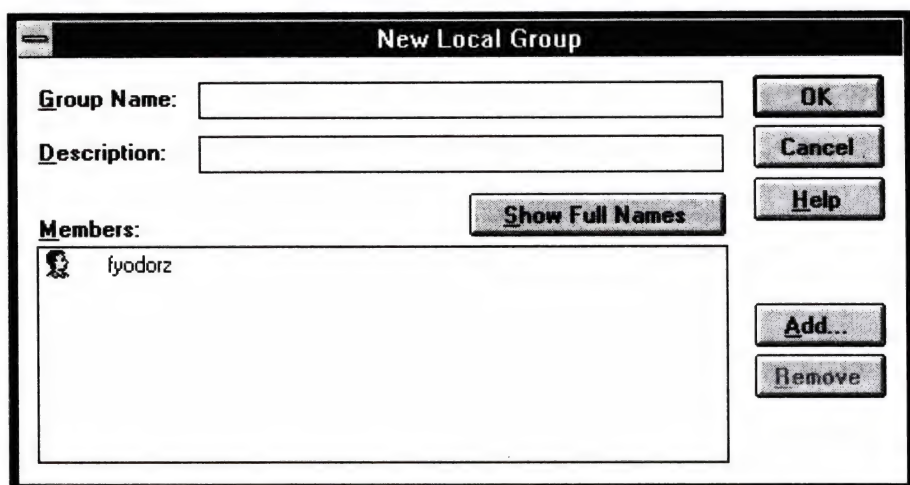
На рисунке в окне **User Manager for Domains** перечислены группы этого домена.



Окно User Manager for Domains.

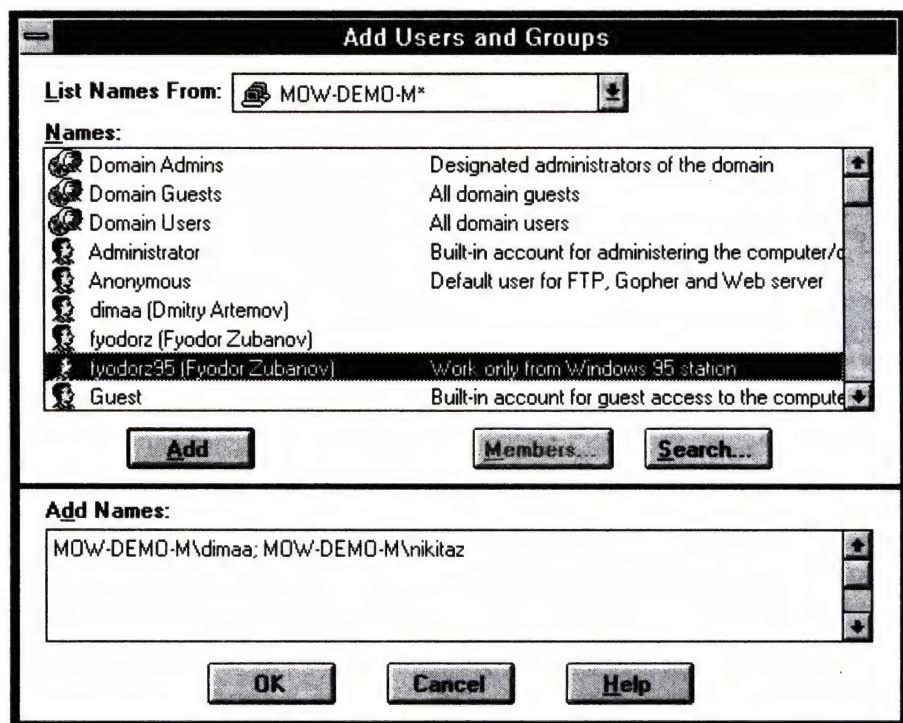
Создание локальной группы

Чтобы создать локальную группу, выберите в меню **User** команду **New Local Group**. В появившемся диалоговом окне укажите имя группы, ее описание и членов группы. Кнопка **Show Full Names** позволяет увидеть полные имена членов группы.



Диалоговое окно *New Local Group*.

Чтобы в группу добавить новых членов, "нажмите" кнопку **Add** — появится такое диалоговое окно:



Диалоговое окно *Add Users and Groups*.

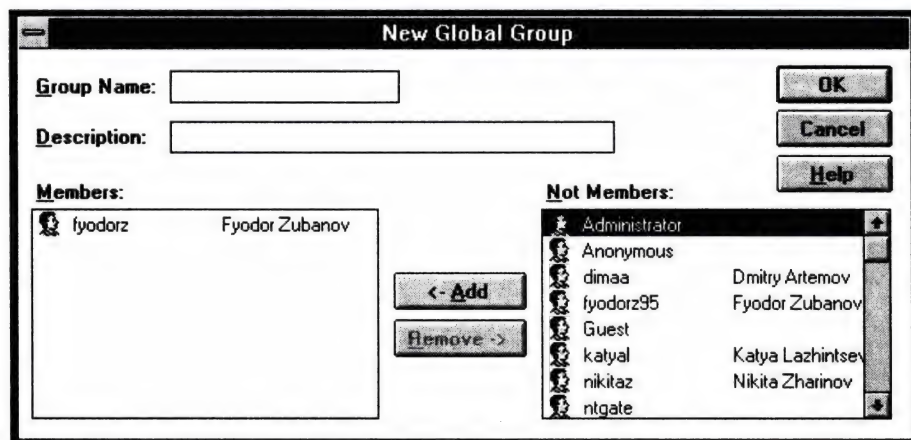
В этом диалоговом окне выберите имя домена, пользователи и глобальные группы которого могут быть включены в локальную группу, а также конкретные имена пользователей и групп. Здесь же выбранные имена добавляются в группу.

Вот кнопки окна *Add Users and Groups*:

Кнопка	Действие
Add	Добавляет имена пользователей или групп, выделенных в списке <i>Names</i> , в список <i>Add Names</i> .
Members	Выводит диалоговое окно <i>Global Group Membership</i> , где перечисляются члены выделенной глобальной группы. Это позволяет выбрать конкретного пользователя из глобальной группы для добавления в локальную.
Search	Выводит диалоговое окно <i>Find Account</i> , где администратор может найти конкретную учетную запись пользователя или группы в этом или других доменах, с которыми установлены доверительные отношения.

Создание глобальной группы

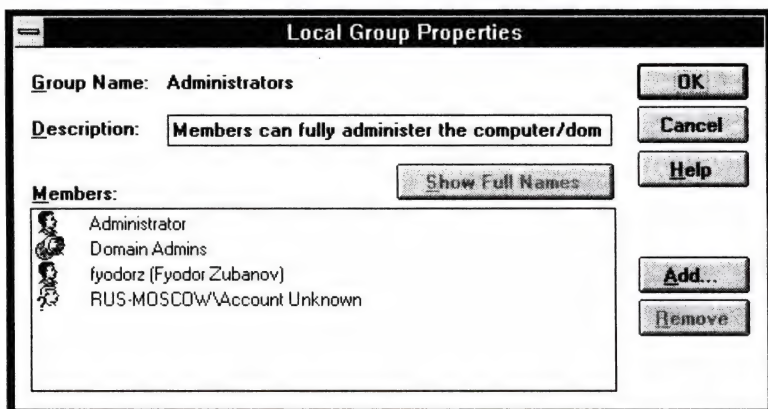
Для создания новой глобальной группы служит команда *New Global Group* меню *User*. Работа с появившимся диалоговым окном аналогична работе с *New Local Group* за тем исключением, что можно оперировать только с учетными записями пользователей одного домена. Щелчок кнопки *Add* добавляет в список *Members* пользователя, выделенного в списке *Not Members*.



Диалоговое окно *New Global Group*.

Модификация локальной группы

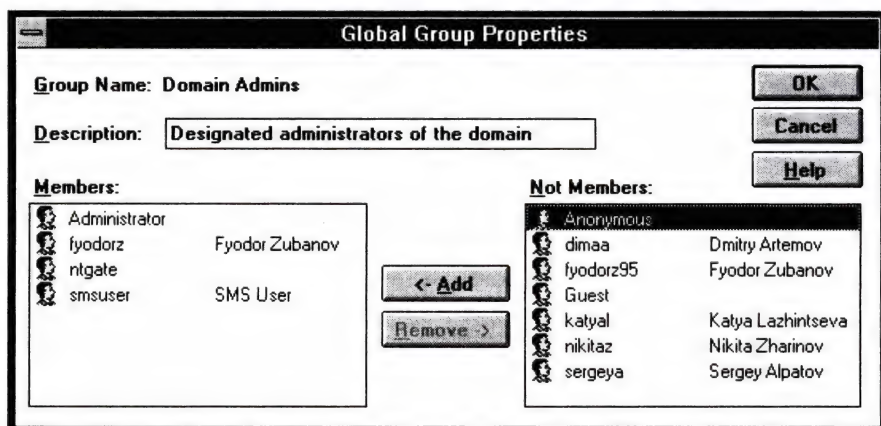
Исключить некоторых членов локальной группы или добавить новых можно в любой момент: выделив имя нужной локальной группы, выберите в меню **User** команду **Properties** или дважды щелкните имя локальной группы. Появится диалоговое окно **Local Group Properties**, сходное с окном **New Local Group**.



Диалоговое окно *Local Group Properties*.

Модификация глобальной группы

Исключить некоторых членов глобальной группы или добавить новых можно в любой момент: выделив имя нужной глобальной группы, выберите в меню **User** команду **Properties** или дважды щелкните имя глобальной группы. Появится диалоговое окно **Global Group Properties**, сходное с окном **New Global Group**.

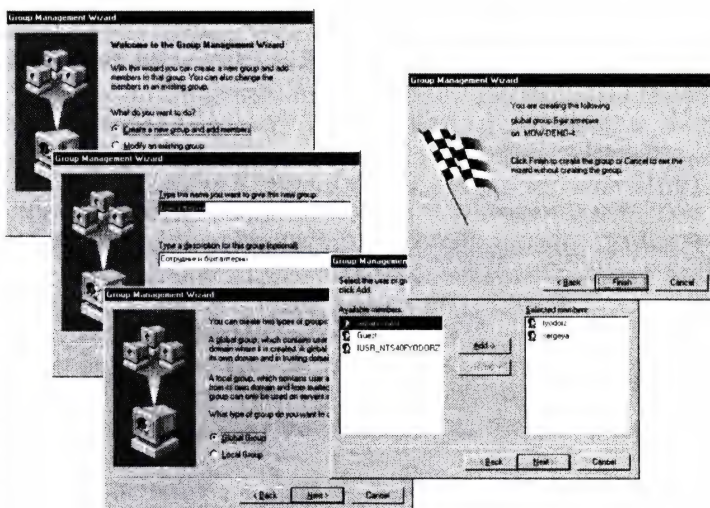


Диалоговое окно *Global Group Properties*.

Создание и модификация групп с помощью программы-мастера Group management Wizard

4.0

В Windows NT Server 4.0 появилась новая программа-мастер, позволяющая безошибочно создавать или модифицировать новые группы в домене или на локальном компьютере. Мало отличаясь функционально от **User Manager** или **User Manager for Domains**, она представляет собой единый инструмент, способный работать как с доменом, так и с отдельно взятым компьютером. Кроме того, пошаговость исполнения с возможностью возврата, заложенная в программы-мастера, гарантирует, что даже начинающий администратор не “натворит дел” в домене. На рисунке показаны некоторые диалоговые окна этой программы.



Шаги создания новой группы в Group Management Wizard.

Специальные группы

Специальные группы создаются операционной системой для особых целей. Эти группы не перечислены в списке **User Manager for Domains**, но могут появляться при присвоении прав на доступ к каталогам, файлам, совместно используемым каталогам и принтерам.

Специальные группы, организуя пользователей в соответствии с тем, как они осуществляют доступ к различным ресурсам, не содержат пользователей в обычном понимании этого термина; администраторы могут не включать в них пользователей. Кто-то становится членом специальной группы по умолчанию, кто-то — в зависимости от активности в сети. В таблице перечислены все специальные группы системы.

<i>Группа</i>	<i>Применяется к</i>
Network	Всем пользователям, подключенным к компьютеру по сети.
Interactive	Любому, кто локально использует компьютер.
Everyone	Любому, кто работает на компьютере независимо от типа доступа. Включает группы Network и Interactive .
Creator Owner	Предоставляет права на доступ создателям подкаталогов, файлов и заданий для печати.
SYSTEM	Операционной системе.

Группа Network

В специальную группу **Network** входит любой пользователь, подключенный к сетевому ресурсу. Если, подключаясь к сетевому ресурсу, пользователь применяет свою собственную либо гостевую учетную запись, он рассматривается как сетевой.

Группа Interactive

Локально зарегистрировавшиеся пользователи автоматически включаются в группу **Interactive**. Члены этой группы осуществляют доступ к ресурсам машины, на которой они фактически работают.

С точки зрения предоставления прав, группы **Interactive** и **Network** различны. Рассмотрим пример. Работая за компьютером А, пользователь осуществляет к его ресурсам локальный доступ. При этом он рассматривается как член группы **Interactive** и имеет назначенные этой группе права. Если тот же пользователь с другого компьютера осуществит по сети доступ к тем же ресурсам на компьютере А, он будет рассматриваться как член группы **Network** с другими правами.

Группа Everyone

В группу **Everyone** автоматически включаются все пользователи, осуществляющие доступ к ресурсам компьютера. Сюда входят гости и пользователи из других доменов, а также группы **Interactive** и **Network**. Администраторы могут назначать этой группе любые права в дополнение к предоставлению прав на доступ к файлам, каталогам, совместно используемым каталогам, принтерам и ключам регистра. Так как любой пользователь по умолчанию является членом группы **Everyone**, администраторы не могут добавлять новые учетные записи в эту группу, но могут исключать группу **Everyone** из списка доступа к тому или иному ресурсу.

Группа Creator Owner

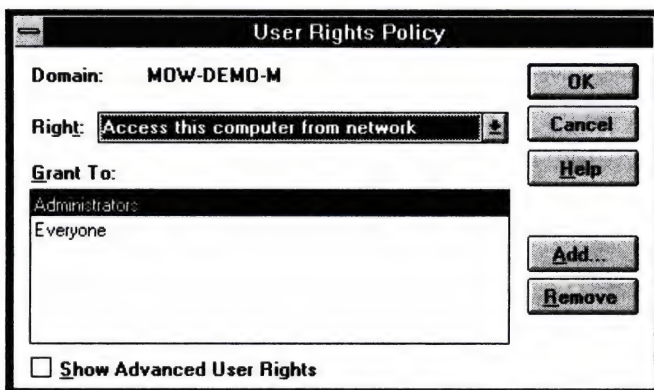
В эту группу входит учетная запись пользователя, создавшего ресурс или взявшего его во владение. На NTFS-разделах права **Creator Owner** назначаются на уровне каталогов. Владелец любых каталогов или файлов внутри такого каталога получит привилегии, назначенные для **Creator Owner**. Эта локальная группа может использоваться для управления правами на доступ к файлам и каталогам, созданным в общедоступной области раздела NTFS.

Права и привилегии пользователей и групп

Выше мы неоднократно упоминали *права* и *привилегии*, присвоенные учетным записям или группам. *Привилегия* — это предоставление пользователю возможности выполнить определенное действие в системе. Привилегии применимы к системе в целом. *Права* — это правила, ассоциированные с определенным объектом (например, файлом, каталогом или принтером). Эти правила устанавливают, какие именно пользователи имеют доступ к объекту и каким образом.

Привилегии имеют приоритет перед правами. Если какой-то пользователь не имеет прав на доступ к некоторому ресурсу, но его группа обладает привилегией доступа ко всем ресурсам системы, то он может осуществить доступ к этому ресурсу.

Привилегии назначаются в диалоговом окне **User Rights Policy** (Политика привилегий), вызываемом в **User Manager for Domains** командой **User Rights** в меню **Policy**.



Диалоговое окно *User Rights Policy*.

В этом диалоговом окне перечислены доступные привилегии, а также пользователи или группы, которым они назначены.

В приведенной ниже таблице перечислены привилегии, которые обычно назначаются различным группам пользователей.

<i>Привилегия</i>	<i>Позволяет пользователям</i>
Access this computer from network	Подключаться к компьютеру по сети.
Add workstations to domain	Добавлять новые рабочие станции в домен.
Back up files and directories	Делать резервное копирование файлов и каталогов. Эта привилегия имеет приоритет перед ограничением прав на доступ к файлам и каталогам.
Change the system time	Устанавливать время внутренних часов компьютера.
Force shutdown from remote system	Зарезервирована.
Load and unload device drivers	Загружать и выгружать драйверы устройств.
Log on locally	Регистрироваться в системе с клавиатуры компьютера.
Manage auditing and security log	Определять, какие типы событий или доступ к каким ресурсам необходимо регистрировать в журнале; просматривать журнал событий и удалять из него записи.
Restore files and directories	Восстанавливать файлы и каталоги. Имеет приоритет перед ограничением прав на доступ к файлам и каталогам.
Shut down the system	Выключать Windows NT Server.
Take ownership of files and other objects	Вступать во владение файлами, каталогами и другими объектами компьютера.

Кроме перечисленных, есть ряд дополнительных привилегий для специальных случаев. Чтобы они появились в списке привилегий диалогового окна, пометьте флажок **Show Advanced User Rights**. Вот они:

<i>Привилегия</i>	<i>Описание</i>
Act as a part of the operating system	Пользователь может работать как защищенная, доверяемая часть операционной системы. Предоставлена некоторым подсистемам. По умолчанию: Никому.
Bypass traverse checking	Пользователь может обходить ветви дерева каталогов. Запрещает доступ пользователям POSIX-приложений. По умолчанию: Никому.
Create a pagefile	Пользователь может создавать страничный файл. (В текущей версии Windows NT Server недоступна.) По умолчанию: Никому.
Create a token object	Для создания меток доступа. Право на это имеет только Local Security Authority. По умолчанию: Никому.

<i>Привилегия</i>	<i>Описание</i>
Create permanent shared objects	Для создания специальных постоянных объектов, таких как \\Device, используемых в Windows NT Server. По умолчанию: Никому.
Debug programs	Пользователь может отлаживать различные низкоуровневые объекты, такие как потоки. По умолчанию: Administrators .
Generate security audits	Для создания входов в журнал регистрации событий защиты. По умолчанию: Никому.
Increase quotas	Для увеличения квот на доступ к объекту (не используется в текущей версии Windows NT Server). По умолчанию: Никому.
Increase scheduling priority	Пользователь может увеличить приоритет процесса. По умолчанию: Administrators , Power Users .
Lock pages in memory	Пользователь может запереть страницы в памяти с тем, чтобы их нельзя было сбрасывать в файл подкачки. По умолчанию: Никому.
Log on as a batch job	Пользователь может регистрироваться через пакетную очередь (в текущей версии Windows NT Server не используется). По умолчанию: Никому.
Log on as a service	Пользователь может выполнять сервисы по защите. По умолчанию: Никому.
Modify firmware environment variables	Пользователь может модифицировать переменные системного окружения (не путать с пользовательским окружением). По умолчанию: Никому.
Profile single process	Пользователю доступны возможности профилирования процессов в Windows NT Server. По умолчанию: Administrators .
Profile system performance	Пользователю доступны возможности профилирования системы в Windows NT Server. По умолчанию: Administrators .
Receive unsolicited device input	Для чтения данных с терминального устройства. По умолчанию: Никому.
Replace a process level token	Для изменения идентификатора доступа процесса. Используется только системой. По умолчанию: Никому.

Привилегии встроенных учетных записей

В Windows NT две встроенные учетные записи: **Guest** и **Administrator**. Они созданы для особых случаев и по умолчанию принадлежат к различным встроенным группам (см. раздел *Группы пользователей*).

Учетная запись Guest

Учетная запись **Guest** служит для однократного доступа в систему или доступа случайных пользователей. По умолчанию он заблокирован и является членом глобальной группы **Domain Guests**. Для этой учетной записи установлен пустой пароль, а его профиль не может отличаться от устанавливаемого по умолчанию. (Подробнее о профилях см. раздел *Профили пользователей*). **Guest** используется как при регистрации по сети, так и локально. Администратор может сконфигурировать каждую рабочую станцию или домен на возможность любого из этих двух видов доступа для гостей либо запретить доступ вообще.

Учетная запись **Guest** требует постоянного внимания. Во-первых, если она разрешена, для нее установлен пустой пароль. Во-вторых, всякий раз при предоставлении прав группе **Everyone** их получает и учетная запись **Guest**. В-третьих, если сделать **Guest** членом группы **Domain Users**, пользователи из недоверяемых доменов получают доступ к ресурсам Вашего домена с привилегиями и правами учетной записи **Guest**.

Чтобы разрешить гостевой вход в систему и локально, и по сети, учетную запись **Guest** нужно разрешить в **User Manager for Domains**. Чтобы разрешить регистрацию гостей только локально, администратор отключает у учетной записи **Guest** привилегию доступа к компьютеру по сети. И наоборот: запрещая для **Guest** локальную регистрацию, администратор разрешает регистрацию по сети.

Управление гостевой учетной записью на Windows NT Workstation выполняется аналогично за тем исключением, что учетная запись **Guest** не заблокирована по умолчанию. Если "гости" нежелательны, администратор ее блокирует.

Учетную запись **Guest** нельзя удалить, но можно переименовать. Если Вы планируете регулярно пользоваться гостевой учетной записью, переименуйте ее, назначьте пароль и разрешайте только по необходимости. Пароль для этой учетной записи не должен быть простым (вроде guest или visitor); регулярно изменяйте его, а права на доступ — проверяйте.

Учетная запись Administrator

Учетная запись **Administrator** позволяет полностью контролировать безопасность и работу системы, в частности контролировать файлы, которыми владеют другие пользователи. Любой знающий имя и пароль административной учетной записи имеет все возможности по администрированию системы.

По умолчанию **Administrator** является членом встроенных групп **Administrators**, **Domain Admins** и **Domain Users** и, таким образом, обладает всеми правами и привилегиями, предоставленными этим группам.

Административная учетная запись назначается для пользователя, управляющего конфигурацией домена. Администраторы, обладая большим контролем над доменом и рабочими станциями в нем, чем другие пользователи, имеют доступ ко всем ресурсам.

Администратор может:

- управлять политикой защиты;
- устанавливать доверительные отношения;
- создавать, изменять или удалять учетные записи пользователей или группы;
- изменять программное обеспечение системы;
- создавать и подключаться к совместно используемым каталогам (в том числе административным);
- устанавливать принтеры и подключаться к ним;
- форматировать разделы жесткого диска;
- выполнять резервное копирование и восстановление файлов;
- отлаживать систему;
- брать во владение файлы и другие объекты;
- устанавливать или обновлять драйверы устройств;
- разблокировать серверы, регистрироваться с серверов и выключать их.

Учетную запись **Administrator** нельзя удалить, но ее можно (и должно!) переименовать. Пароль этой учетной записи нельзя забыть: ведь единственная возможность его восстановления — переустановка системы Windows NT. **Administrator** нельзя исключить из групп **Administrators**, **Domain Admins** и **Guests**.

Административная учетная запись — объект постоянного внимания: столько у нее прав и привилегий! Потеря ее равнозначна концу света. Используйте эту

учетную запись только в административных целях. Она должна быть доступна только для администратора. Если же какой-то иной пользователь нуждается в тех или иных привилегиях, включите его учетную запись в соответствующую группу (о привилегиях групп см. ниже).

Например, на время отсутствия администратор Федор назначает Дмитрия для управления учетными записями пользователей. При создании учетной записи Дмитрий включается в группу **Account Operators**, что позволяет ему управлять учетными записями пользователей, не выполняя других административных функций.

Привилегии встроенных локальных групп

В Windows NT несколько типов встроенных локальных групп, привилегии которых рассмотрены далее.

Привилегии группы Users

Любой, кто регулярно работает с компьютером, должен иметь учетную запись в группе **Users**. Пользователь, зарегистрировавшийся в системе как член группы **Users**, может:

- выключать систему;
- запускать приложения;
- управлять файлами;
- создавать новые локальные группы;
- управлять локальными группами;
- иметь персональный профиль (например, цвета в системе, шрифты и т.п.);
- подключаться к компьютеру по сети;
- регистрироваться локально.

Учетные записи локальной группы **Users** — это обычные пользователи компьютера или сети. Большинство учетных записей, создаваемых администратором, должны принадлежать к этой группе.

Пользователи из локальной группы **Users** на Windows NT Workstation могут:

- регистрироваться на рабочей станции и использовать ее для доступа в сеть;
- блокировать и выключать рабочую станцию;
- иметь профиль на рабочей станции;
- создавать и удалять локальные группы на рабочей станции.

Пользователи должны беречь свой пароль, как военную тайну: избегайте очевидных паролей, нигде не записывайте и не произносите вслух! Пользовательские учетные записи должны иметь такие характеристики, как ограничение времени работы и способов использования учетной записи.

Привилегии группы **Power Users**

Группа **Power Users** предоставляет возможность выполнять административные функции без возможности полного контроля над системой.

Член группы **Power Users** может делать все, что и член группы **Users**, плюс:

- предоставлять каталоги в совместное использование в сети и отменять его;
- устанавливать, управлять и предоставлять в совместное использование принтеры;
- создавать новые, неадминистративные учетные записи пользователей;
- модифицировать те учетные записи, что были созданы;
- удалять учетные записи пользователей;
- включать учетные записи пользователей на рабочей станции во встроенные группы **Power Users**, **Users** и **Guests**;
- устанавливать внутренний таймер компьютера;
- выключать систему с удаленного узла;
- профилировать производительность;
- увеличивать приоритеты;
- предоставлять в совместное использование файлы и принтеры на рабочей станции.

Группа **Power Users** существует только на Windows NT Workstation. Поэтому самый общий подход — включить учетные записи пользователей домена в группу **Power Users** на их собственных рабочих станциях. Например, администратор может включить пользователя Dima в группу **Power Users** на его рабочей станции, оставив его в группе **Domain Users** в домене. Dima сможет предоставлять ресурсы в совместное использование и управлять системой на своей рабочей станции, оставаясь рядовым пользователем домена.

Для каждой рабочей станции администратор должен решить, включать ли учетную запись пользователя домена в группу **Power Users** (для большего контроля) или в группу **Users** (для меньшего). Чтобы не предоставлять ресурсы рабочих станций в совместное использование, администратор не добавит свою учетную запись в группу **Power Users**.

Привилегии группы Administrators

Группа Administrators на Windows NT Workstation предоставляет возможность полного контроля над системой. Пользователь рабочей станции, включенный в группу **Administrators**, может создавать, удалять и редактировать учетные записи пользователей и локальные группы, предоставлять для совместного доступа каталоги и принтеры, предоставлять права и привилегии пользователям, устанавливать системные файлы и программы на рабочую станцию.

Заметьте: в отличие от администраторов сетей типа Netware, администраторы Windows NT автоматически не имеют прав на доступ ко всем файлам на сервере. Если доступ к какому-то файлу запрещен, администратор должен сначала взять этот файл во владение и только потом осуществить доступ. При этом первоначальному владельцу файл вернуть нельзя. Поэтому у администраторов нет средств для модификации файла, к которому у них изначально нет доступа, так чтобы это не стало известно владельцу файла.

У любого файла на NTFS-разделе есть свой владелец, который может ограничить к нему доступ. Каждый вновь создаваемый файл принадлежит создателю. Так что конфиденциальная информация защищена и от администратора.

Члены группы **Administrators** на Windows NT Workstation обладают следующими привилегиями в дополнение к имеющимся у пользователей группы **Power Users**:

- изменять и удалять учетные записи пользователей и групп, созданных другими;
- назначать учетные записи пользователей в группы по умолчанию;
- создавать, удалять и подключаться к административным ресурсам совместного использования;
- преодолевать блокировку рабочих станций;
- создавать разделы на жестком диске и форматировать его;
- назначать права пользователям;
- контролировать аудит;
- выполнять резервное копирование и восстанавливать всю систему;
- отлаживать систему;
- вступать во владение файлами и другими объектами.

Пользователи из группы **Administrators** на Windows NT Server полностью контролируют домен. Они могут выполнять практически любые административные функции на машинах, входящих в домен: создавать, удалять и модифицировать локальные и глобальные группы, учетные записи пользователей, предоставлять совместный доступ к каталогам и принтерам, предоставлять пользователям привилегии и права на доступ к ресурсам, устанавливать системные файлы и приложения на удаленных рабочих станциях, записывать и отписывать сервер, форматировать жесткие диски на сервере и создавать общие группы.

Привилегии группы Guests

По умолчанию учетная запись **Guest** позволяет любому пользователю, не имеющему своей учетной записи на компьютере или в домене, осуществить доступ к нему как локально, так и по сети.

Сетевое программное обеспечение часто использует **Guest** для доступа к компьютеру, поэтому в системе рекомендуется иметь эту учетную запись. Так как любой работающий под именем **Guest** имеет возможность доступа к сетевым ресурсам, внимательно следите за предоставлением прав доступа к ресурсам.

У гостей компьютера меньше возможностей, чем у обычных пользователей. Пользователи группы **Users** могут иметь свой собственный профиль, записывать рабочую станцию, создавать, удалять и редактировать локальные группы на рабочих станциях, в то время как члены группы **Guests** — нет.

Привилегии группы Backup Operators

Члены данной группы могут выполнять резервное копирование файлов и их восстановление. Любой пользователь может выполнять резервное копирование и восстановление только тех файлов, право доступа к которым он имеет. Члены группы **Backup Operators** могут резервировать и восстанавливать любые файлы независимо от того, имеют они права доступа к ним или нет. Но они не могут прочитать файлы, к которым у них закрыт доступ.

Привилегии группы Server Operators

Члены группы **Server Operators** могут управлять серверами домена, например, создавать, удалять и модифицировать принтеры, предоставляемые на сервере в совместное использование, выполнять резервное копирование и восстановление файлов, удалять и изменять совместно используемые каталоги, форматировать жесткие диски на сервере, изменять системное время. Члены этой группы могут регистрироваться непосредственно на серверах и выключать серверы.

Привилегии группы Account Operators

Члены группы **Account Operators** могут через **User Manager for Domains** создавать, изменять и удалять большинство учетных записей пользователей и групп в домене. Члены **Account Operators** имеют возможность регистрироваться непосредственно на сервере, выключать сервер и через **Server Manager** добавлять компьютеры в домен.

Привилегии группы Print Operators

Члены группы **Print Operators** могут создавать, удалять и модифицировать принтеры, предоставляемые в совместное использование. Они могут регистрироваться непосредственно на сервере и выключать сервер.

В таблице обобщены привилегии локальных групп Windows NT Workstation:

	Administrators	Power User	Users	Guests	Everyone	Backup Operators
Привилегии						
Регистрироваться локально	✓	✓	✓	✓	✓	✓
Осуществлять доступ к компьютеру по сети	✓	✓			✓	
Вступать во владение файлами	✓					
Управлять журналом аудита и защиты	✓					
Изменять системное время	✓	✓				
Выключать систему	✓	✓	✓		✓	✓
Выключать систему с удаленного компьютера	✓	✓				
Выполнять резервное копирование файлов и каталогов	✓					✓
Восстанавливать файлы и каталоги	✓					✓
Встроенные возможности						
Создавать и редактировать учетные записи пользователей	✓	✓				
Создавать и редактировать локальные группы	✓	✓	✓			
Назначать привилегии пользователям	✓					
Запирать рабочую станцию	✓	✓			✓	
Отпирать рабочую станцию	✓					
Форматировать жесткий диск рабочей станции	✓					
Создавать общие группы	✓	✓				
Иметь локальный профиль	✓	✓				✓
Предоставлять каталоги в совместное использование	✓	✓				
Предоставлять принтеры в совместное использование	✓	✓				

В следующей таблице обобщены возможности и привилегии пользователей встроенных локальных групп на Windows NT Server:

	Administrators	Server Operators	Account Operators	Print Operators	Backup Operators	Console Operators	Replicator	Everyone	Users	Guests
Привилегии										
Регистрироваться локально	✓	✓	✓	✓	✓	✓				
Осуществлять доступ к компьютеру по сети	✓					✓		✓		
Вступать во владение файлами	✓									
Управлять журналом аудита и защиты	✓					✓				
Изменять системное время	✓	✓				✓				
Выключать систему	✓	✓	✓	✓	✓					
Выключать систему с удаленного компьютера	✓	✓								
Выполнять резервное копирование файлов и каталогов	✓	✓			✓	✓				
Восстанавливать файлы и каталоги	✓	✓			✓	✓				
Встроенные возможности										
Создавать и редактировать учетные записи пользователей	✓		✓							
Создавать и редактировать глобальные группы	✓		✓							
Создавать и редактировать локальные группы	✓		✓							✓
Назначать привилегии пользователям	✓									
Запирать сервер	✓	✓						✓		
Отпирать сервер, запертый другими		✓								
Форматировать жесткий диск сервера	✓	✓								
Создавать общие группы	✓	✓								
Иметь локальный профиль	✓	✓	✓	✓	✓					
Предоставлять каталоги в совместное использование	✓	✓								
Предоставлять принтеры в совместное использование	✓	✓		✓						

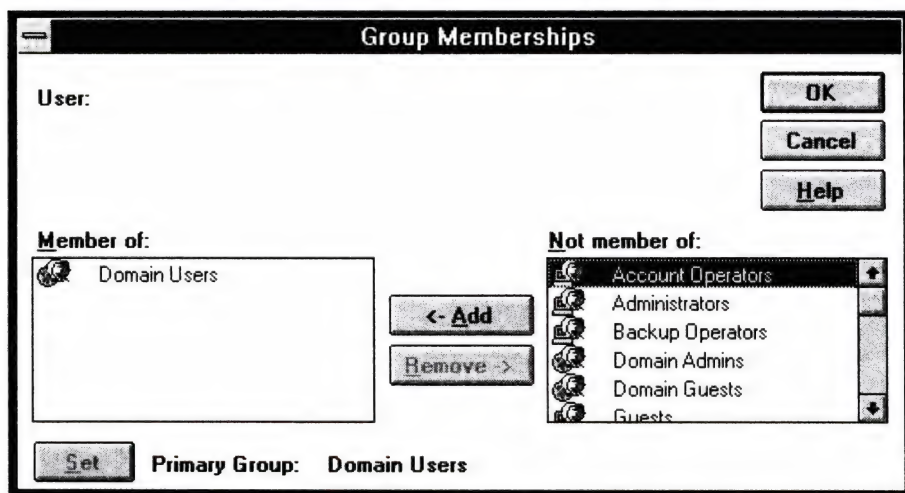
Изменение привилегий пользователей

Итак, любой пользователь в Windows NT принадлежит к какой-либо — встроенной или созданной впоследствии — группе, чем определяются его привилегии и права. Но любой пользователь может быть наделен дополнительными правами и привилегиями, отсутствующими в тех группах, куда он входит.

Включение пользователей в группы

Быстро изменить привилегии и права можно, включив пользователя в различные группы. Администратор узнает, какие привилегии имеет пользователь, посмотрев, какими привилегиями обладают группы, членом которых является пользователь.

Управляются группы через *User Manager* или *User Manager for Domains*, где сначала надо выбрать имя пользователя, затем — команду *Properties* из меню *User*; после щелчка кнопки *Groups* появится окно *Group Memberships*.



Диалоговое окно *Group Memberships*.

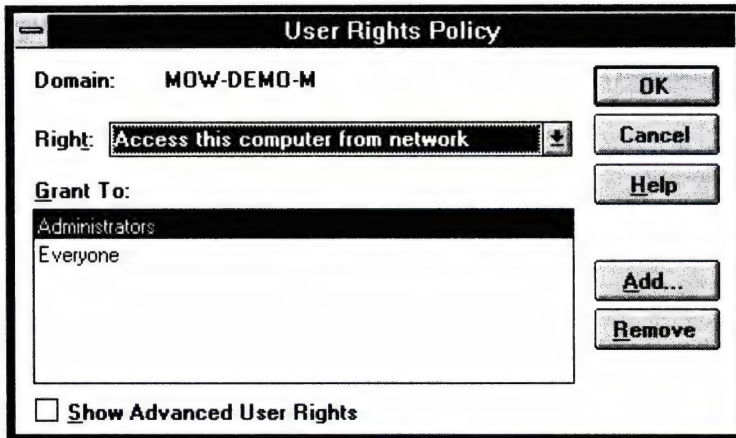
В списке *Member of* перечислены группы, членом которых является выбранный пользователь, а в списке *Not Member of* — все группы системы, в которые его можно включить. Выделив в правом списке группу и щелкнув кнопку *Add*, учетную запись пользователя включают в выбранную группу и тем самым присваивают новые привилегии.

В нижней части диалогового окна отмечена первичная группа (*Primary Group*), к которой принадлежит пользователь. Она используется *Windows NT Services for Macintosh* или выполняемыми POSIX-приложениями. В первичную группу могут входить только глобальные группы.

Изменение определенных привилегий пользователя

Хотя описанный выше способ назначения привилегий и прав пользователям — самый удобный и рекомендуемый, есть еще один (аналогичный назначению привилегий группам) — непосредственное назначение привилегий.

Непосредственного назначения привилегий также осуществляется через **User Manager** или **User Manager for Domains**, только в меню **Policies** надо выбрать команду **User Rights**. Из списка появившегося диалогового окна выберите привилегию, которой должен обладать пользователь, щелкните кнопку **Add** и выберите нужное имя учетной записи пользователя.



Окно *User Rights Policy*.

Этот метод целесообразен, например, если пользователю надо временно разрешить выполнить на сервере определенную операцию. Допустим, в филиале нет своего технического персонала, но есть сотрудник, способный выполнять задачи по администрированию системы. В головном же подразделении принято решение увеличить емкость жесткого диска на сервере в филиале путем добавления новых дисков и объединения их в единый том. С этой целью сотруднику филиала временно назначаются соответствующие привилегии, позволяющие выполнять операции с диском, но запрещающие прочие административные функции.

В общем случае, однако, данный метод не рекомендуется, так как при этом отсутствует общая картина назначенных привилегий и легко забыть о каком-нибудь пользователе, подвергнув тем самым безопасность системы большому риску.

Профили пользователей

Профилем пользователя называется файл с информацией о персональных настройках рабочей среды пользователя, загружаемый при регистрации. Для администратора профили — одно из мощнейших средств управления средой пользователя.

Каждый раз, когда пользователь Windows NT Workstation регистрируется в системе или домене, на его компьютере восстанавливаются все параметры среды в

том виде, в каком они были в момент окончания предыдущего сеанса работы. При выходе пользователя из системы все изменения в настройках, сделанные им в процессе работы, заносятся в файл профиля [кроме пользователей, зарегистрировавшихся в системе как гость (учетная запись **Guest**)].

В профиле пользователя хранятся такие параметры, как установки **Program Manager, File Manager, Print Manager, Control Panel**, командной строки, инструментария, приложений для Windows и ссылки в системе справки. В таблице детализированы установки по каждому из разделов.

<i>Источник</i>	<i>Сохраняемые параметры</i>
Program Manager	Определяемые пользователем установки для Program Manager , включая персональные группы программ и их свойства, программные элементы и их свойства, все установки, сохраняемые по командам Save Settings on Exit и Save Settings Now .
File Manager	Определяемые пользователем установки для File Manager , включая сетевые подключения и все сохраняемые командой Save Settings on Exit .
командная строка	Определяемые пользователем установки для командной строки, включая цвета, размер буфера экрана и его положение.
Print Manager	Подключаемые сетевые принтеры и все параметры, сохраняемые командой Save Settings on Exit .
Control Panel	Все установки разделов Color, Mouse, Desktop, Cursor, Keyboard, International, Sound . Из раздела System сохраняются только переменные окружения (User Environment Variables). В остальных разделах панели управления не содержится информация, специфичная для конкретного пользователя.
Accessories	Определяемые пользователем установки, влияющие на конфигурацию Windows NT Server. В Accessories входят Calculator, Calendar, Cardfile, Clock, Notepad, Paintbrush и Terminal .
Приложения для Windows сторонних фирм	Любое приложение, написанное специально для Windows NT, может отслеживать информацию о настройках, специфичную для каждого пользователя. Эта информация также сохраняется в профиле пользователя.
Ссылки в системе справки	Любые закладки, размещенные в системе справки Windows NT.

В защищенной среде для разных видов работ можно создать различные профили, назначаемые затем пользователям для выполнения соответствующих работ. Профили также применяются для обеспечения нескольким пользователям одинаковой рабочей среды. Это может быть либо профиль, устанавливаемый по умолчанию, либо специфичный профиль.

Профили, устанавливаемые на рабочих станциях, превращают Windows NT Workstation в реальную многопользовательскую систему: у любого сотрудника, зарегистрировавшегося на рабочей станции будет своя рабочая среда. Применение профилей упрощает администрирование и повышает уровень защищенности. Предположим, администратор системы отдела разработчиков Дмитрий, создав профиль, хранящийся в совместно используемом каталоге на сервере, назначил его всем разработчикам. Если разработчикам понадобится новая программа, то, чтобы каждый не выполнял ее установку, Дмитрий один раз создаст значок этого приложения и сохранит в общем профиле. После этого оно будет доступно всем разработчикам.

Обязательные и персональные профили

По умолчанию для каждого пользователя Windows NT (кроме Guest) поддерживается свой профиль. Профили делятся на обязательные, персональные и профили по умолчанию.

Если назначен *обязательный профиль*, изменения, внесенные пользователем в процессе работы, в профиле не сохраняются, и в следующий раз при его регистрации в системе восстановятся параметры обязательного профиля. Так как обязательные профили нельзя изменять, они лучше всего подходят для гостевых учетных записей.

Если назначен *персональный профиль*, все изменения, внесенные пользователем в течение сеанса работы, сохраняются в профиле и воспроизводятся при следующей регистрации в системе. Этот профиль можно сохранить на сервере в совместно используемом каталоге, что позволяет сотруднику, зарегистрировавшемуся на любой рабочей станции, иметь свою персональную среду работы.

Профиль умолчания — стандартный профиль Windows NT — применяется, если:

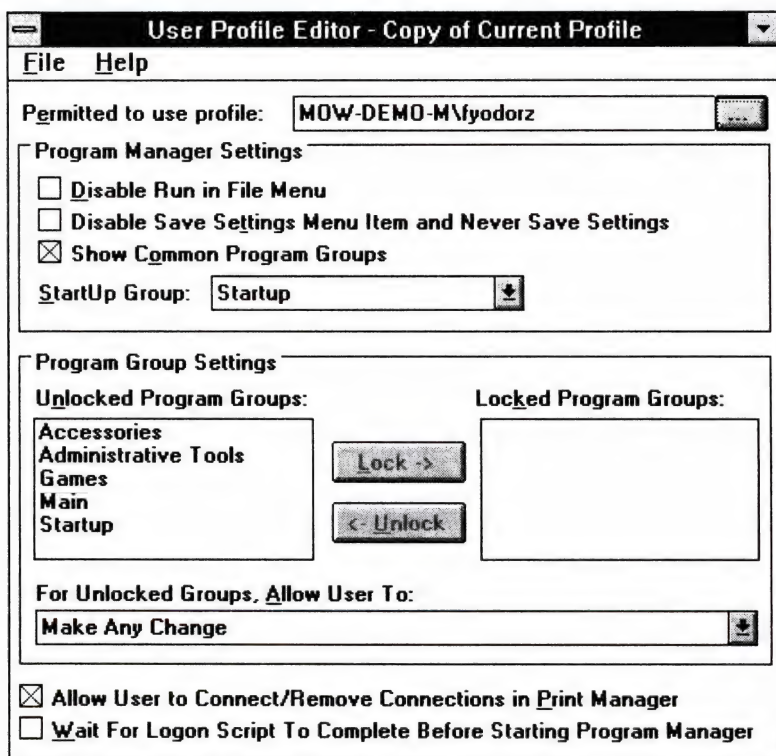
- у пользователя нет персонального профиля;
- пользователь еще ни разу не регистрировался в системе;
- к персональному профилю нет доступа в момент регистрации;
- пользователь регистрируется как гость.

Пользователь может изменить профиль умолчания, и изменения будут отслежены системой (кроме гостевых учетных записей). Если при следующей регистрации не будет других доступных профилей, измененный профиль умолчания станет персональным профилем данного пользователя.

Когда в системе никто не зарегистрирован, появляется *системный профиль умолчания*. В это время вводное диалоговое окно предложит нажать комбинацию клавиш Ctrl+Alt+Del. В системном профиле умолчания также сохраняются цвет фона, обои и хранители экрана.

Создание и редактирование профилей

Профили создаются и редактируются с помощью утилиты **User Profile Editor** (ее значок находится в группе **Administrative Tools** в Windows NT Server). Эта программа используется только членом локальной группы **Administrators** или глобальной группы **Domain Admins**.



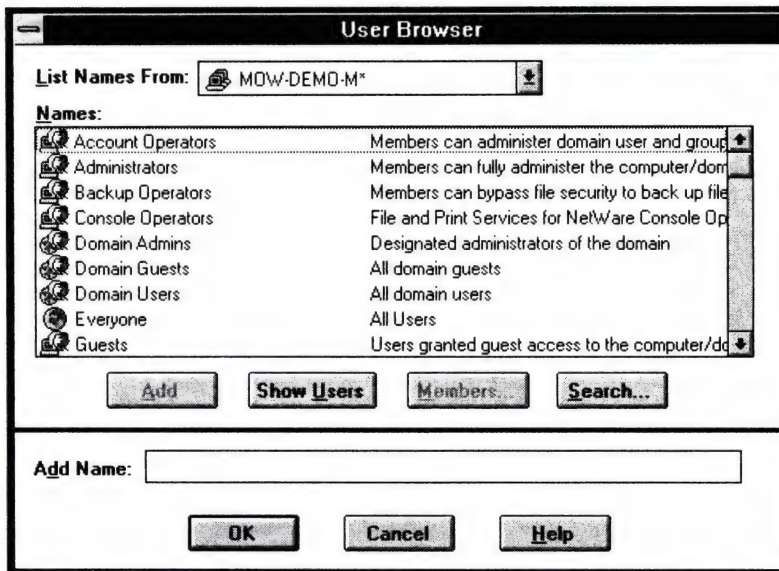
Окно User Profile Editor.

User Profile Editor состоит из нескольких секций, назначение которых описано ниже.

Permitted to use this profile

В этой секции указывается определенный пользователь или локальная или глобальная группа, имеющая доступ к этому профилю. Скажем, если администратор Саша назначит этот профиль Никите, то при следующей регистрации Никите будет предоставлен неявный доступ к этому профилю.

Щелчок кнопки просмотра пользователей (она расположена рядом с этим полем) раскрывает список пользователей и групп в домене вроде показанного на рисунке ниже.



Диалоговое окно просмотра списка пользователей User Browser.

Установки Program Manager

Данный раздел позволяет:

- > определить приложения, которые будут запущены при старте **Program Manager**;
- > запретить пользователю доступ к общим группам;
- > запретить использование команды **Run** в меню **File**;
- > запретить сохранять сделанные изменения в профиле.

Хотя пользователю запрещено выполнять команду **Run**, он сможет запускать приложения из других мест — **File Manager**, командной строки или при изменении свойств программных элементов в **Program Manager**.

Установки Program Group

Этот раздел позволяет определить, в каких программных группах пользователю разрешено делать изменения, а в каких нет. Администратор может указать, ка-

кие именно изменения применимы к группам. В таблице перечислены возможные комбинации изменений, доступных пользователю.

Выбрано	Что может пользователь
Make Any Change	Создавать, удалять и модифицировать программные элементы и группы программ.
Create/Delete/Change Program Items	Создавать, удалять и модифицировать программные элементы (но не группы программ).
Change All Program Items Properties	Изменять (но не создавать или удалять) программные элементы. Пользователь не может создавать, изменять или удалять группы программ.
Change Program Item Properties Except Command Line	Изменять любые свойства программных элементов, кроме командной строки. Пользователь не может создавать или удалять программные элементы, а также создавать, удалять или модифицировать группы программ.

Разрешение пользователю делать подключения в Print Manager

Данная опция позволяет пользователю подключаться к сетевым принтерам через **Print Manager**. Если администратор запретит кому-либо подключения, все попытки такого пользователя вывести документ на сетевой принтер окажутся безуспешными.

Необходимость ожидания завершения отработки сценария регистрации (Logon Script) до запуска Program Manager

Данный параметр позволяет завершить отработку сценария регистрации до запуска **Program Manager**. Полезно устанавливать в том случае, если в процессе отработки должны выполняться обязательные приложения, способные в той или иной степени установить права и рабочую среду пользователя.

Сохранение профиля

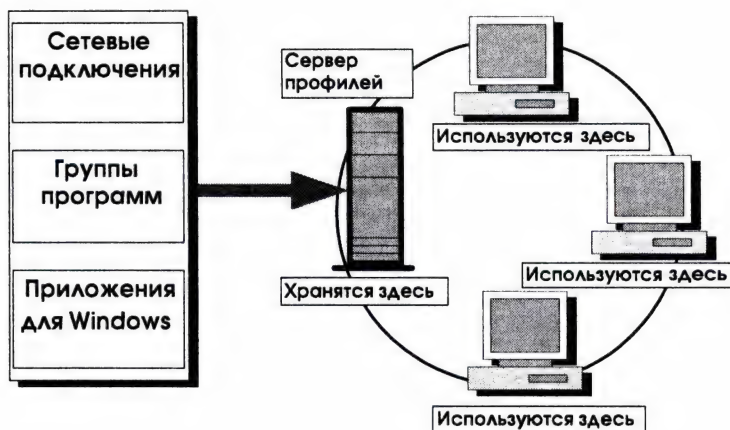
Профили сохраняются в реестре. Они распознаются по имени пользователя и воссоздают условия окончания последнего сеанса работы. Профили всех пользователей на этой рабочей станции различны. Поэтому любой из них может вносить в профиль изменения, которые и будут воссозданы в новом сеансе.

Так как профили хранятся в реестре, профиль пользователя, регистрирующегося на рабочей станции, зависит от того, где он регистрировался раньше: здесь или на сервере.

Если первое, используется локальный профиль этой рабочей станции. При переходе с одной станции на другую используются локальные профили каждой из них.

Серверные профили делятся на персональные (модифицируемые каждым пользователем) и обязательные (применяемые в системах с высокой степенью защищенности). Эти профили хранятся в реестре на сервере.

Серверные профили



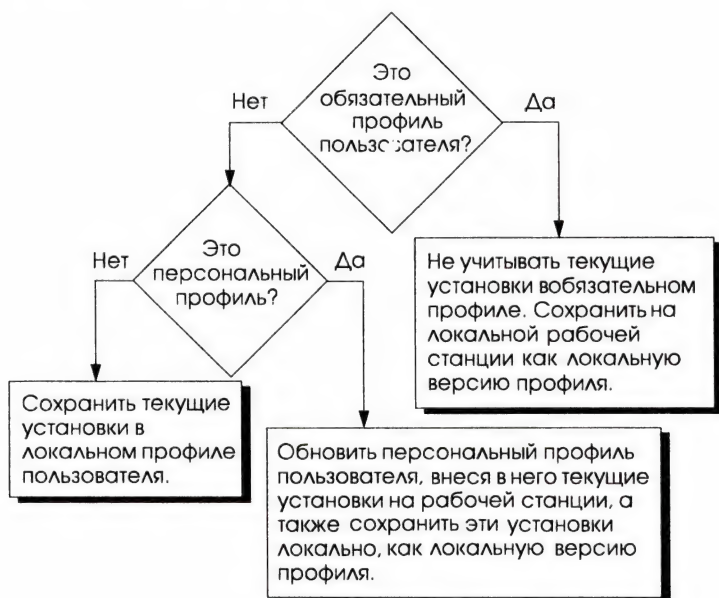
Существуют три причины использования серверных профилей:

1. Положение каждого серверного профиля указано в базе учетных записей домена для каждого пользователя. Независимо от того, на каком сервере он регистрируется, пользователь будет применять один и тот же профиль. Другими словами, профиль следует за пользователем.
2. Администратор сети может создать профиль для ограничения доступа пользователя к рабочей станции и запрета изменений среды на рабочей станции.
3. Ряду пользователей можно назначить обязательный профиль. При этом администратор, изменяя всего лишь один профиль, может изменять доступ ряда пользователей к приложениям.

Профили пользователей находятся в каталогах:

- > *Профиль умолчания.* \<корень winnt>\SYSTEM32\CONFIG\USERDEF
- > *Локальный профиль.* \<корень winnt>\SYSTEM32\CONFIG\<имя пользователя>
- > *Серверный профиль.* На локальном жестком диске или в совместно используемом каталоге там, где это указано в базе учетных записей.

При выходе пользователя из системы Windows NT определяет, был ли профиль обязательным или нет. Если да, то внесенные пользователем изменения игнорируются, нет — изменения сохраняются в профиле текущего пользователя.



Сохранение профилей.

Кроме автоматического сохранения в реестре, профили, созданные в **User Profile Editor**, можно сохранять в файлах, присвоив одно из расширений: **USR** — для персональных и **MAN** — для обязательных профилей. В дальнейшем администратор выбирает тот или иной файл профиля и назначает его пользователям. Это заметно упрощает работу администратора.

Домашние каталоги — персональные хранилища

Администратор может назначить *домашний каталог* каждому пользователю в качестве места хранения персональных файлов. Такой каталог становится открываемым по умолчанию в диалоговых окнах **File Open** и **File Save As**, в командной строке и во всех приложениях, где нет специально определяемого рабочего каталога.

Если на рабочей станции есть дисковое пространство, администратор может разрешить доступ пользователю к этому пространству, запретив доступ к остальным ресурсам. Администратор может сконфигурировать рабочую станцию, так чтобы домашний каталог на ней был единственным, для которого у пользователя будут назначены права доступа, отличные от **No Access**.

При запуске командной строки в ней откроется домашний каталог. Также в любом приложении, для которого нельзя специально установить рабочий каталог, домашний каталог будет рабочим. Если домашний каталог находится не на локальной рабочей станции, а где-то в сети, то автоматически будет устанавливаться необходимое сетевое соединение всякий раз при регистрации пользователя.

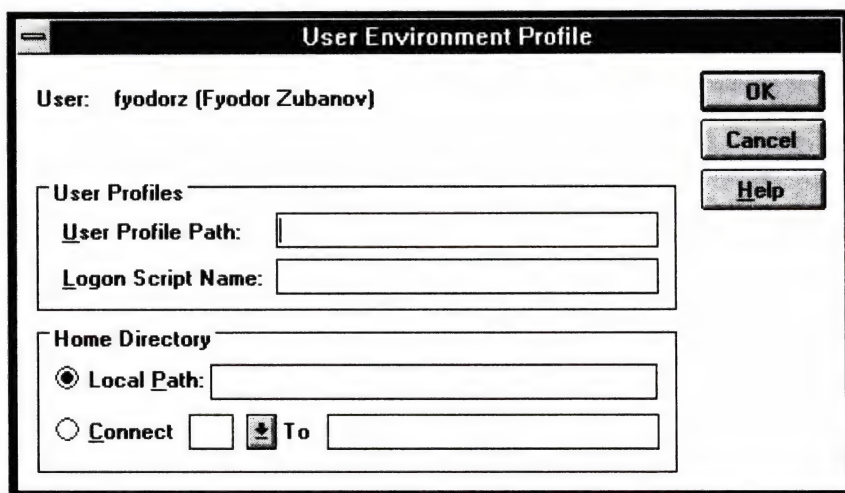
Определяя домашний каталог, можно указать либо на какой-нибудь общий каталог, либо на особый для каждого пользователя. При этом можно применять универсальные соглашения об именах (UNC), скажем, в виде `\\SERVER\USERS\DIMA`. Чтобы создать каталог для каждого пользователя, администратору придется попотеть, зато он получит больший контроль, да и для пользователей это гораздо удобнее.

По умолчанию домашний каталог пользователя — `\USERS\DEFAULT` — находится на том диске, где установлена операционная система. Его можно изменить на другой локальный или совместно используемый каталог на сервере. Если пользователь принадлежит домену, установите домашний каталог на сервере. Если рассматривается локальная учетная запись рабочей станции, домашний каталог рекомендуется создавать на рабочей станции.

Домашние каталоги автоматически генерируются двумя способами:

1. **User Manager for Domains** автоматически создаст домашний каталог, если при создании учетной записи в домене указать совместно используемый сетевой каталог. Если создать каталог нельзя, появится сообщение о необходимости создания такого каталога вручную. Если при администрировании доменной учетной записи как домашний указан локальный каталог, он не будет создан автоматически.
2. **User Manager for Domains** пытается создать указанный домашний каталог, если администрируется локальная база учетных записей на рабочей станции. Если каталог создать невозможно, появится сообщение о необходимости создать его вручную. В Windows NT Workstation можно администрировать с помощью **User Manager for Domains**, выбрав команду **Select Domain** и указав имя рабочей станции вместо имени домена.

Если домашний каталог находится в разделе NTFS, установите соответствующие права на доступ к этому каталогу. При автоматическом создании домашнего каталога **User Manager for Domains** предоставит права полного доступа (**Full Control**) к нему только пользователю, для которого он создан. Если один и тот же каталог назначен как домашний одновременно двум и большему числу пользователей, полный доступ к нему получит группа **Everyone**. Если каталог уже существует, **User Manager for Domains** не изменяет права на доступ к нему. В таком случае права на доступ назначаются с помощью **File Manager**.



Диалоговое окно *User Environment Profile*.

Сценарий регистрации и домашний каталог назначаются пользователю в диалоговом окне ***User Environment Profile*** в ***User Manager***. При обращении к домашнему каталогу в Windows NT используются следующие подменяемые величины:

- %HOMEPATH% — имя пути к домашнему каталогу пользователя;
- %HOMEDRIVE% — имя локального диска, к которому подключается домашний каталог, расположенный в сети;
- %HOMESHARE% — универсальное наименование (UMC) совместно используемого в сети каталога, в котором находится домашний каталог.

Сразу нескольким пользователям домашний каталог назначается так же, как одному: выделив в ***User Manager*** нужных пользователей, выберите в меню ***Users*** команду ***Properties***. Щелкнув кнопку ***Profile***, укажите в диалоговом окне в поле ***Home Directory*** соответствующий каталог, где вместо конкретного имени пользователя введите %USERNAME%.

Сценарии регистрации (Logon Scripts)

Сценариями регистрации являются командные файлы, назначенные пользователям. Сценарием регистрации может быть текстовый файл с расширением .CMD или .BAT или исполняемый файл с расширением .EXE. Эти файлы исполняются при регистрации пользователя. Сценарий регистрации может включать в себя подключение к сетевым устройствам, конфигурирование среды пользователя или запуск того или иного приложения. Заметьте: сценарии регистрации выполняются *после* регистрации пользователя в системе.

С помощью сценариев администратор устанавливает единый механизм регистрации в сети. Сценарии могут быть персонифицированными или одинаковыми для ряда пользователей и обычно применяются при сетевых подключениях и запуске служебных программ.

Сценарии регистрации не столь универсальны, как профили. Профиль позволяет выполнять все, что и сценарий, плюс дополнительные функции. Но есть ряд причин, по которым применять сценарии регистрации необходимо. Их используют:

- вместо профилей на рабочих станциях, работающих в MS-DOS;
- для управления только частью профиля пользователя;
- для выполнения сетевых подключений, общих для ряда пользователей.

Кроме того, сценарии:

- проще создавать и редактировать;
- могут тиражироваться на любой сервер, т.е. они будут автоматически доступны на любом сервере.

Сценарии регистрации назначаются пользователем в диалоговом окне **User Environment Profile** и хранятся на его компьютере в каталоге, устанавливаемом по умолчанию. Для системы Windows NT это:

```
C:\WINNT35\SYSTEM32\REPL\IMPORT\SCRIPTS
```

Если Windows NT Server является частью сети, сценарии регистрации могут располагаться в каталогах, содержимое которых тиражируется на другие серверы (см. раздел *Тиражирование каталогов*). По умолчанию сценарий записывается в каталог:

```
C:\WINNT35\SYSTEM32\REPL\EXPORT\SCRIPTS
```

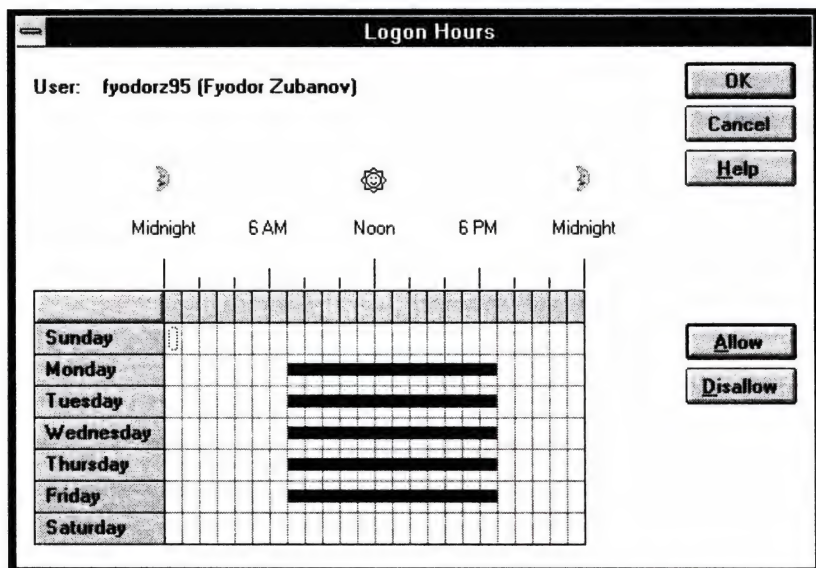
Чтобы повысить защищенность, храните сценарии регистрации на разделах NTFS, а доступ к ним ограничьте через **File Manager**.

Чтобы сценарии регистрации работали на всех серверах в домене, администратор должен позаботиться о том, чтобы сервис **Replicator** был запущен на всех серверах домена и тиражирование выполнялось между указанными каталогами.

Ограничение времени работы пользователей

Чтобы установить больший контроль над пользователями, администратор может ограничить время их работы с сетевыми ресурсами. Например, разрешить работу в сети только по будням с 9 до 18 часов.

Часы работы устанавливаются в диалоговом окне **Users Properties**. Щелчок кнопки **Hours** выведет на экран диалоговое окно **Logon Hours**.



Диалоговое окно *Logon Hours*.

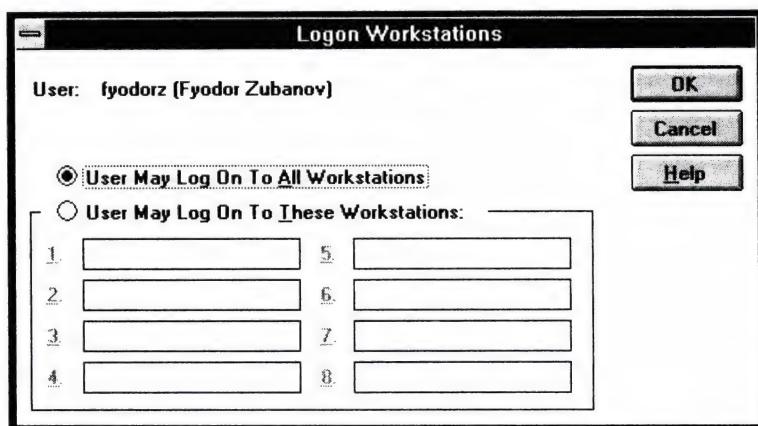
По умолчанию регистрация разрешена 24 часа в сутки 7 дней в неделю. Чтобы запретить работу на определенное время, выделите его и щелкните кнопку **Disallow**.

Ограничение времени регистрации влияет лишь на доступ пользователя в сеть, но не на возможность работы на рабочей станции.

Поведение системы по истечении разрешенного времени зависит от глобальных параметров, описываемых в диалоговом окне **Account Policies** (см. раздел *Глобальные параметры, влияющие на защищенность системы*).

Ограничение числа рабочих станций, с которых возможна регистрация

Администратор может ограничить число рабочих станций, с которых пользователь регистрируется в системе. По умолчанию пользователю разрешено регистрироваться с любой рабочей станции. Для ввода ограничений щелкните кнопку **Logon To** в диалоговом окне **Users Properties**.



Диалоговое окно *Logon Workstations*.

В появившемся диалоговом окне перечислите имена разрешенных рабочих станций.

Вводить ограничения имеет смысл, если конкретный пользователь должен иметь доступ к особо конфиденциальной информации. В этом случае стоит разрешить доступ к ней только с тех станций, на которых приняты повышенные меры безопасности. Это могут быть станции без гибких дисков, с защищенным от вскрытия корпусом и т.п.

Использование Редактора системной политики в Windows NT Server 4.0

4.0

- Как уже говорилось, профили пользователей, определяемые через **User Profile Editor**, действительны только для тех, кто работает на компьютерах с установленной Windows NT. Для всех остальных операционных систем приходится применять сценарии регистрации. Но в операционной системе Windows 95 существует понятие профиля пользователя, аналогичное используемому в Windows NT. Вот почему в Windows NT Server 4.0 появился инструмент, заимствованный в Windows 95 и позволяющий гибко формировать профили как для всех работающих в системе, так и для определенных пользователей, — **System Policy Editor** (Редактор системной политики). Располагается он в группе **Administrative Tools**.
- Редактор системной политики позволяет определять политику по отношению к пользователям и к компьютерам с установленной Windows NT или Windows 95. Функции редактора охватывают все возможности как уже рассмотренных средств администрирования, так и инструментов, описанных далее в этой главе.

Системная политика по отношению к пользователям

Все элементы политики применяемой по отношению к пользователям, входящим в домен, делятся на следующие категории:

- **Control Panel (Панель управления).** Определяет политику, предотвращающую доступ пользователя к настройкам параметров дисплея в *Control Panel*.
- **Desktop (Рабочий стол).** Принудительно устанавливает оформление рабочего стола (цветовые схемы, обои).
- **Shell (Оболочка).** Устанавливает ограничения на элементы интерфейса, содержимое некоторых папок и возможность сохранения модификаций профиля.
- **System (Система).** Устанавливает ограничения на использование средств редактирования реестра и запуск программ.
- **Windows NT Shell (Оболочка Windows NT).** Позволяет полностью переопределить содержимое папок, значки, используемые для их отображения на рабочем столе, а также устанавливает ограничения на применение расширений оболочки и общих групп программ.
- **Windows NT System (Система Windows NT).** Позволяет определять переменные окружения для пользователя.

Эти элементы политики можно применять по умолчанию для всех пользователей домена, для отдельных пользователей домена или групп, а также для локальных пользователей. Подробно об этих элементах сказано далее в этой главе.

Системная политика по отношению к компьютерам

Редактор системной политики позволяет определять значения параметров как для всех компьютеров, входящих в домен, так и для отдельно взятых компьютеров. Параметры, определенные для компьютера по умолчанию, применяются при регистрации на компьютере нового пользователя, по отношению к которому пока не проводится системная политика.

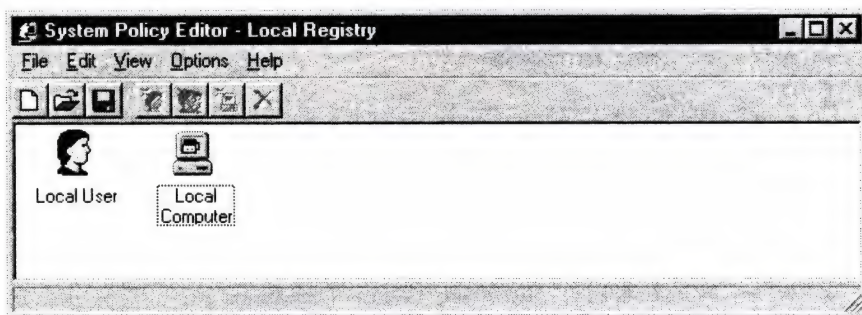
Элементы политики, проводимой по отношению к компьютеру, делятся на такие категории:

- ▶ **Network (Сеть).** Устанавливает правила назначения системной политики.
- ▶ **System (Система).** Устанавливает параметры, необходимые для осуществления управления по протоколу SNMP, а также определяет приложения, запускаемые при старте системы.
- ▶ **Windows NT Network (Сеть Windows NT).** Ограничивает использование административных каталогов, предоставляемых для совместного доступа.
- ▶ **Windows NT System (Система Windows NT).** Указывает правила регистрации на компьютере, использование возможностей файловой системы, а также параметры доступа по протоколу FTP.
- ▶ **Windows NT Printers (Принтеры Windows NT).** Устанавливает параметры печати: приоритет, информацию о доступности принтера и сообщения об ошибках печати.
- ▶ **Windows NT Remote Access. (Удаленный доступ Windows NT).** Определяет некоторые, наиболее общие параметры удаленного доступа.
- ▶ **Windows NT User Profiles (Профили пользователей Windows NT).** Определяет параметры при работе пользователя в "медленных" сетях.

Два режима работы Редактора системной политики

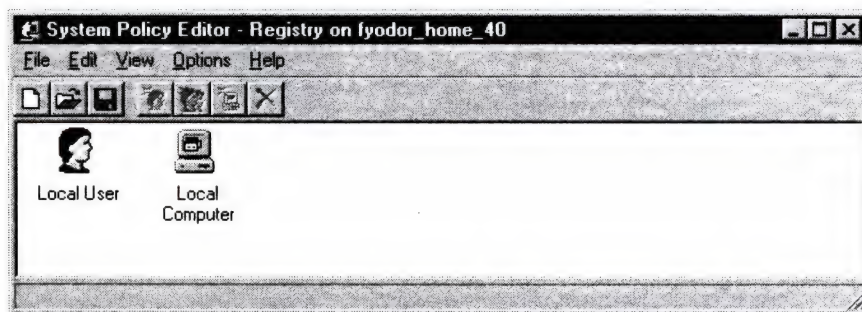
Редактор системной политики работает в двух режимах: *реестра* и *файла политики*. В первом можно непосредственно редактировать значения, хранящиеся в реестре локального или любого удаленного компьютера. Все изменения сразу вступают в силу. Во втором режиме можно создавать и модифицировать файлы системной политики (расширение .POL). При этом реестр редактируется косвенно, а изменения вступают в силу только во время регистрации пользователя на компьютере.

Чтобы работать в режиме реестра, в **System Policy Editor** выберите в меню **File** команду **Open Registry** (для модификации параметров в реестре локального компьютера) или команду **Connect** (для модификации параметров в реестре удаленного компьютера). В первом случае сразу откроется такое окно:



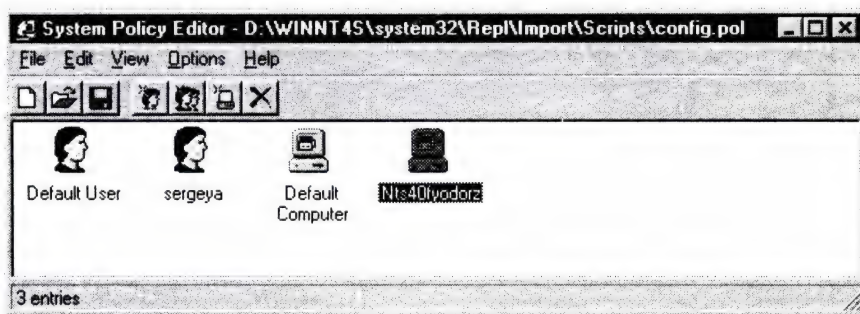
Два значка соответствуют параметрам локального пользователя (**Local User**) и локального компьютера (**Local Computer**). Обратите внимание на заголовок окна — **Local Registry** (Локальный реестр).

Если Вы решили редактировать реестр удаленного компьютера, вызвав команду **Connect**, Вам будет предложено выбрать одного из пользователей, подключенных к этому компьютеру (обычно это всего один пользователь), чьи параметры в реестре Вы хотите редактировать. Укажите нужное имя, и появится диалоговое окно:

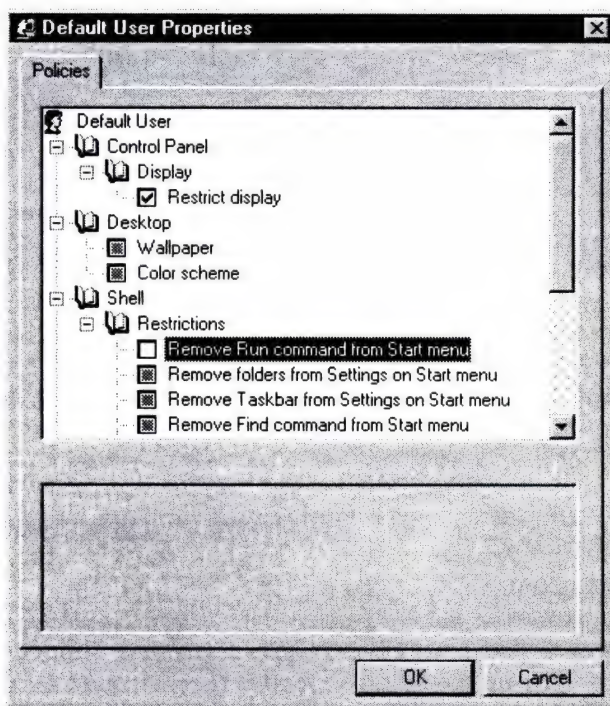


От описанного ранее оно отличается лишь заголовком *Registry on <имя компьютера>*.

Для работы в режиме редактирования файла политики в меню **File** выберите команду **Open Policy** (Открыть файл политики) или **New Policy** (Новый файл политики). Появится диалоговое окно с именем редактируемого файла политики в заголовке.



Чтобы отредактировать параметры, устанавливаемые по умолчанию для всех пользователей или всех компьютеров, дважды щелкните значок **Default User** или **Default Computer**. В появившемся диалоговом окне будет представлено дерево параметров и значения, соответствующие параметрам. Значения отображаются в виде флажков, каждый из которых может быть в одном из трех состояний: отмечен, не отмечен, заштрихован.



- Отмеченный флажок соответствует тому параметру, который будет применен в политике, неотмеченный — параметру, действие которого отменено, а заштрихованный — параметру, значение которого не изменялось с момента предыдущего редактирования. "Третье состояние" позволяет не думать обо всех параметрах, а устанавливать только необходимые.

Два вида загрузки системной политики

Системная политика может быть загружена на рабочую станцию автоматически или принудительно. Для *автоматической* загрузки файл системной политики должен располагаться на сервере в строго определенном месте и иметь определенное имя. Файл политики должен храниться в:

\\главный контроллер домена\netlogon\config.pol.

— для клиентов Windows 95 и

\\главный контроллер домена\netlogon\ntconfig.pol.

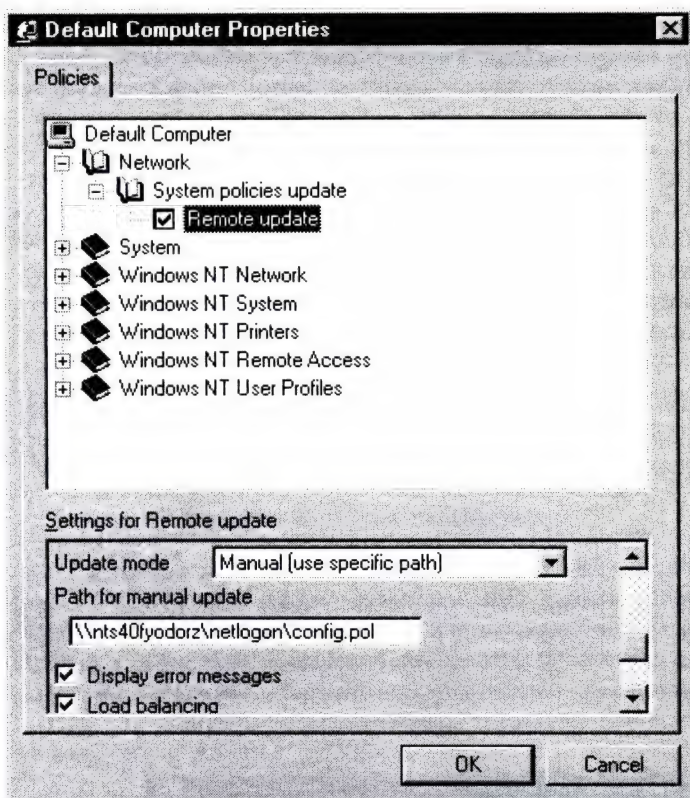
— для клиентов Windows NT.

Понятно, что в системе с несколькими контроллерами домена регистрация пользователя может быть выполнена любым из них. Чтобы сработала автоматическая загрузка политики, необходимо обеспечить *тиражирование* файла **config.pol** на другие контроллеры домена.

Если Вы планируете применить разную системную политику к разным пользователям и/или компьютерам в сети, можно определить для них отдельные файлы политики, которые будут загружаться *принудительно*. Эти файлы могут лежать в произвольных местах (даже локально на рабочих станциях) и определяются параметром **Remote update**. Для его модификации дважды щелкните значок **Local Computer** или значок выбранного компьютера, затем в разделе **Network** раскройте ветвь **System policies update** и отметьте флажок **Remote update**. В нижней части диалогового окна (см. рисунок) укажите вид загрузки (**Update mode**): **Manual (Use specific path)**, а чуть ниже укажите полный путь к файлу политики в формате UNC.



Замечание: На удаленном клиенте должен работать сервис Microsoft Remote Registry, должно быть разрешено удаленное администрирование и активизирована защита на уровне пользователя (для Windows 95).



В крупных сетях при одновременном входе в систему тысяч пользователей, обращающихся к одному файлу политики, производительность сети может заметно снизиться. Чтобы уменьшить нагрузку на контроллер домена, отметьте флажок **Load Balancing** (Балансировка загрузки) на всех контроллерах домена, используемых для регистрации пользователей и содержащих файл системной политики.

Групповая политика

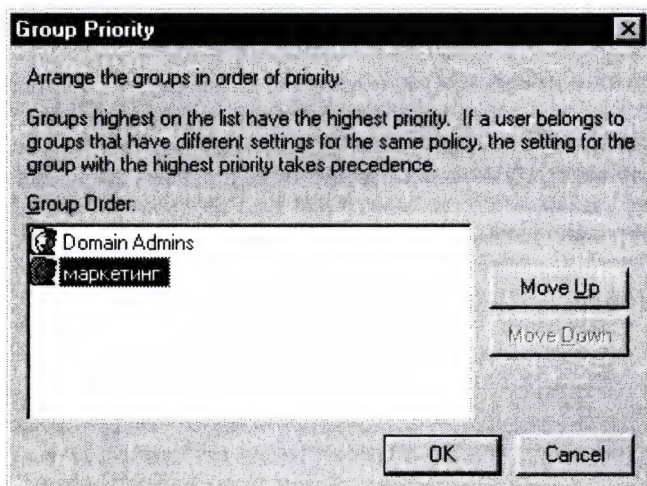
Для удобства управления большим числом пользователей можно устанавливать системную политику для групп. При этом применяются *глобальные группы* домена, определенные в **User Manager for Domains**. Чтобы включить ту или иную группу в файл системной политики, выберите в меню **Edit** команду **Add Group** и укажите в списке имя нужной глобальной группы домена. Можно указать имя другого домена и группу из него.

Когда значок группы появится в диалоговом окне Редактора системной политики, дважды щелкните его и устанавливайте необходимые параметры точно так, как это делалось для отдельного пользователя.

Политика, определенная для нескольких групп, будет загружаться, начиная с групп с наименьшим *приоритетом*. Обработаются все группы, но группа с наивысшим приоритетом — в последнюю очередь, поэтому, если пользователь принадлежит сразу к нескольким группам, то параметры, закрепленные за группой с более высоким приоритетом, приводят к замене соответствующих параметров для групп с более низким приоритетом.

Замечание: Если к какому-то пользователю, входящему в группу, применяется своя системная политика, групповая политика на него не распространяется.

Кто же устанавливает приоритеты для групп? Конечно, администратор домена либо лицо с соответствующими полномочиями. Для установки приоритетов в меню **Options** выберите команду **Group Priority**. В появившемся диалоговом окне будут перечислены глобальные группы, охваченные системной политикой. Выделяя ту или иную группу и щелкая кнопки **Move up** (передвинуть выше) или **Move down** (передвинуть ниже), изменяют относительный приоритет групп.



На приведенном рисунке у группы **Domain Admins** приоритет выше, чем у группы **Маркетинг**. Системная политика запрещает членам группы **Маркетинг** изменять конфигурацию рабочего стола, изменять цвето-

- вую гамму и заставки экрана, но разрешает все это членам группы
- **Domain Admins**. Допустим, Юрий принадлежит к обеим группам. В та-
- ком случае даже несмотря на то, что членам группы **Marketing** запре-
- щено изменять настройки рабочего стола, Юрий сможет это сделать, так
- как на группу **Domain Admins** это ограничение не распространяется.

Параметры системной политики

- В этом разделе перечислены параметры системной политики, которые
- можно установить в Windows NT по умолчанию. Они определяются шаб-
- лонами WINNT.ADM и COMMON.ADM (подробнее о шаблонах см. далее).
- Параметры перечислены в порядке их появления в окне **System Policy**
- **Editor**. В этой книге не приведены параметры, задаваемые для Windows
- 95 (определяются шаблоном WINDOWS.ADM). Полное их описание со-
- держится в книге Ресурсы Windows 95.

Параметры, специфичные для пользователя

- Как указывалось выше, для пользователя имеются следующие категории
- параметров: **Control Panel**, **Desktop**, **Shell**, **System**, **Windows NT Shell**,
- **Windows NT System**. Далее в таблицах приведено описание каждого из
- параметров по категориям. В описании ограничений, как правило, указы-
- вается, как пользователь может обойти то или иное ограничение. Адми-
- нистратор должен накладывать ограничения весьма внимательно и “при-
- крывать” всевозможные “лазейки”.

Параметры Панели управления (Control Panel)

Параметр	Описание
Control Panel — Display — Restrict display	Ограничение возможностей настройки экрана
Deny access to display icon (Запретить доступ к значку Display)	Запрещает доступ к значку Display в Control Panel .
Hide Background tab (Скрыть вкладку Background)	Скрывает вкладку Background (Фон) диалогового окна Display Properties .
Hide Screen Saver Tab (Скрыть вкладку Screen Saver)	Скрывает вкладку Screen Saver (Заставка) диалогового окна Display Properties .
Hide Appearance Tab (Скрыть вкладку Appearance)	Скрывает вкладку Appearance (Оформление) диалогового окна Display Properties .
Hide Settings Tab (Скрыть вкладку Settings)	Скрывает вкладку Settings (Параметры) диалогового окна Display Properties .

Параметры рабочего стола (Desktop)

Параметр	Описание
----------	----------

Wallpaper (Обои)	Если отмечен этот флажок, то в качестве фонового рисунка устанавливается указанное растровое изображение. Если отмечен флажок Tile Wallpaper , указанное растровое изображение равномерно заполняет весь фон экрана.
Color Scheme (Схема цветов)	Если отмечен этот флажок, используется указанная схема цветов.

Параметры оболочки (Shell)

Параметр	Описание
Remove Run Command from Start menu (Исключить команду RUN из меню Start)	Удаляет команду RUN из меню Start . Однако это не мешает пользователю запускать приложения другим способом (скажем, из командной строки).
Remove folders from Settings on Start menu (Удалить папки из меню Settings)	Запрещает доступ к разделу Settings (Настройки) в меню Start . Тем не менее доступ к отдельным элементам этого раздела возможен из других мест.
Remove Taskbar from Settings on Start menu (Удалить команду Taskbar из меню Settings)	Запрещает вызов настройки параметров Панели задач из меню Start . При этом щелчок правой кнопкой мыши Панели задач с последующим выбором в меню команды Properties вызывает диалоговое окно настройки.
Remove Find command from Start menu (Удалить команду Find из меню Start)	Запрещает использование команды Find (Поиск) в меню Start . Если установлен клиент MSN, вызов аналогичной функции в нем не запрещен.
Hide drives in My Computer (Скрыть диски в папке My Computer)	Запрещает доступ к дискам в папке My Computer . Запустив File Manager , можно получить обычный доступ ко всем дискам.
Hide Network Neighborhood (Скрыть значок папки Network Neighborhood)	Запрещает доступ к сети в папке Network Neighborhood . Доступ через File Manager по-прежнему не ограничен.
No Entire Network in Network Neighborhood (Скрыть пункт Entire Network в папке Network Neighborhood)	Запрещает просмотр структуры всей сети в папке Network Neighborhood . Просмотр средствами File Manager тем не менее возможен.
No workgroup contents in Network Neighborhood (Отсутствие рабочих групп в папке Network Neighborhood)	Запрещает показ состава рабочих групп в папке Network Neighborhood . Просмотр средствами File Manager тем не менее возможен.

Параметры оболочки (Shell) (продолжение)

Параметр	Описание
Hide all items on desktop (Скрыть все объекты на рабочем столе)	Запрещает доступ ко всем объектам на рабочем столе.
Disable Shutdown command (запретить команду Shutdown)	Запрещает выполнение команды Shut Down (Завершение работы) и выводит соответствующее пояснение.
Don't save settings on exit (не сохранять параметры настройки при выходе)	Запрещает сохранение параметров на диске. Аналогичен по действию обязательному профилю пользователя.

Параметры системы (System)

Параметр	Описание
Disable Registry Editing Tools (Запретить использование средств редактирования Реестра)	Запрещает доступ к редактору реестра, но не запрещает доступ к режиму работы Registry в System Policy Editor .
Run Only Allowed Windows applications (Разрешить исполнение только определенных программ для Windows)	Запрещает запуск любых приложений для Windows, кроме указанных Вами. Проверка осуществляется по имени исполняемого файла. Поэтому самые сообразительные пользователи смогут запускать "недозволенные" программы, переименовав их файлы.

Параметры оболочки Windows NT (Windows NT Shell)

Параметр	Описание
Custom Folders	Собственные папки
Custom Programs folder (Папка Programs)	Изменяет содержимое каталога Programs. Укажите путь к этому каталогу, содержащему исполняемые или LNK-файлы
Custom desktop icons (Значки на рабочем столе)	Переопределяет значки на рабочем столе. Укажите путь к каталогу, в котором лежат исполняемые или LNK-файлы.
Hide Start menu subfolders (Скрыть папки, вложенные в меню Start)	Этот параметр устанавливается, если у Вас собственная папка Programs . В противном случае у пользователя появятся два раздела Programs .
Custom Startup folder (Папка Startup)	Изменяет содержимое каталога Startup . Укажите путь к каталогу, в котором лежат исполняемые или LNK-файлы
Custom Network Neighborhood (Папка Network Neighborhood)	Изменяет содержимое каталога Network Neighborhood . Укажите путь к каталогу, где лежат исполняемые или LNK-файлы и который включается в сетевое окружение.

Параметры оболочки Windows NT (Windows NT Shell) (продолжение)

Параметр	Описание
Custom Start menu (Папка Start menu)	Изменяет структуру меню Start . Необходимо указать путь к каталогу, в котором лежат исполняемые или LNK-файлы, определяющие новое меню.
Custom shared Programs folder (Совместно используемая папка Programs)	Изменяет содержимое совместно используемого каталога Programs . Укажите путь к этому каталогу, содержащему исполняемые или LNK-файлы.
Custom shared desktop icons (Совместно используемые значки на рабочем столе)	Переопределяет значки на рабочем столе. Укажите путь к совместно используемому каталогу, в котором лежат исполняемые или LNK-файлы.
Custom shared Start menu (Совместно используемая папка Start menu)	Изменяет структуру совместно используемого меню Start . Укажите путь к каталогу, в котором лежат исполняемые или LNK-файлы, определяющие новое меню.
Custom shared Startup folder (Совместно используемая папка Startup)	Изменяет содержимое совместно используемого каталога Startup . Укажите путь к каталогу, в котором лежат исполняемые или LNK-файлы.
Restrictions	Ограничения
Only use approved shell extensions (Использовать разрешенные расширения оболочки)	Не позволяет пользователям работать с непроверенными расширениями оболочки, способными вызвать дополнительную загрузку служб поддержки.
Remove common program groups from Start menu (Удалить общие группы программ из меню Start)	Удаляет общие программы, позволяя пользователю запускать только его личные приложения (например, открывать файл MDB, но не запускать Microsoft Access).

Параметры системы Windows NT (Windows NT System)

Параметры	Описание
Parse AUTOEXEC.BAT (Просматривать файл AUTOEXEC.BAT)	Когда отмечен этот флажок, параметры окружения, описанные в файле AUTOEXEC.BAT, добавляются к параметрам окружения пользователя.

Параметры, специфичные для компьютера

- Выше говорилось, что для пользователя имеются следующие категории параметров: **Network, System, Windows NT Network, Windows NT System, Windows NT Printers, Windows NT Remote Access, Windows NT User Profiles**. В следующих таблицах приведены описания параметров по категориям

Параметры сети (Network)

Параметр	Описание
System policies update — Remote update (Обновление системной политики — Удаленное обновление)	<p>Если отмечен этот флажок, обновление политики выполняется по следующим правилам:</p> <p>Update Mode — определяет, должна ли системная политика загружаться автоматически (выбирается по умолчанию) или вручную.</p> <p>Path for manual update — определяет полный путь к файлу (записанный через UNC) системной политики в случае ручной загрузки политики.</p> <p>Display Error messages — если отмечен этот флажок, пользователю выводятся сообщения об ошибках загрузки системной политики.</p> <p>Load balance — если отмечен этот флажок, происходит балансировка процесса загрузки: файлы политики загружаются не только с главного контроллера домена, но и с тех серверов, на которых выполняется аутентификация пользователя.</p>

Параметры системы (System)

Параметр	Описание
SNMP	
Communities (сообщества)	Указывает одну или несколько групп хост-компьютеров, к которым относится данный компьютер. Предназначен для администрирования с использованием SNMP. Этим сообществам разрешается обращаться к агенту SNMP.
Permitted Managers (Управляющие)	Указывает IP- или IPX-адреса, по которым разрешено получать информацию от агентов SNMP. Если этот параметр не определен, любые SNMP-консоли могут обращаться к агенту.
Traps for public community (Перехваты для сообщества Public)	Указывает IP- или IPX-адреса тех хост-компьютеров в сообществе Public , которым Вы хотите пересылать перехваты от сервиса SNMP.
Run	
Run (Загружать при запуске)	Определяет, какие приложения или утилиты выполняются при регистрации пользователя. Щелкните кнопку Show для редактирования списка этих приложений.
Run once (Однократно загружать при запуске)	Определяет, какие приложения или утилиты однократно выполняются при регистрации пользователя. Щелкните кнопку Show для редактирования списка этих приложений.

Параметры сети Windows NT (Windows NT Network)

Параметр	Описание
Sharing	
Create hidden drive shares (Workstation) (Создавать скрытые совместно используемые ресурсы — рабочая станция)	Если отмечен этот флажок, при запуске рабочей станции автоматически создаются ресурсы вида <имя диска>\$ и Admin\$. Наличие таких ресурсов снижает защищенность системы, так что сбросьте этот флажок.
Create hidden drive shares (Server) (Создавать скрытые совместно используемые ресурсы — сервер)	Если отмечен этот флажок, то при запуске сервера автоматически создаются ресурсы вида <имя диска>\$ и Admin\$. Наличие таких ресурсов снижает защищенность системы, так что сбросьте этот флажок.

Параметры системы Windows NT (Windows NT System)

Параметр	Описание
Logon	Регистрация
Logon banner (Заставка при регистрации)	Позволяет указать заголовок и текст сообщения, выводимого при регистрации пользователя. Назначение аналогично предупреждению о легальности использования. (Подробнее см. главу <i>Система безопасности Windows NT</i> .)
Automatic logon (Автоматическая регистрация)	Позволяет автоматически загружать систему. Для этого укажите имя учетной записи, которая будет использоваться для регистрации, и соответствующий пароль. Такой способ регистрации сильно снижает защищенность системы (см. раздел <i>Автоматическая регистрация</i> в главе <i>Система безопасности Windows NT</i> , где объяснено, в каких случаях его использовать).
Enable shutdown from Authentication dialog box (Разрешение терминировать систему из диалогового окна Authentication)	Когда отмечен этот флажок в диалоговом окне Authentication доступна кнопка Shutdown. По умолчанию она недоступна в Windows NT Server и доступна в Windows NT Workstation.
Do not display last logged on user name (Не показывать имя предыдущего пользователя)	Когда этот флажок отмечен, в диалоговом окне Authentication не отображается имя последнего зарегистрировавшегося пользователя. В целях повышения защиты рекомендуется этот флажок отмечать.
File System	Файловая система
Do not create 8.3 file names for long file names (Не создавать файлов формата 8.3 для длинных имен файлов)	По умолчанию каждому файлу, имеющему длинное имя, соответствует еще одно имя в формате 8.3. Если в сети нет клиентов, не умеющих работать с длинными именами файлов (например, DOS или Windows 3.x), можно отметить этот флажок.
Allow extended characters in 8.3 file names (Разрешить использование расширенных символов в именах файлов формата 8.3)	Если отмечен этот флажок, то в коротких именах файлов могут использоваться символы национальных алфавитов (например, русские). Следует помнить, что если на клиенте не установлена соответствующая кодовая страница (866 для русского языка), то их доступ к таким файлам будет невозможен (см. главу <i>Файловые системы и разграничение доступа к файлам и каталогам</i>).

Параметры системы Windows NT (Windows NT System) (продолжение)

Параметр	Описание
Do not update last access time (Не обновлять время последнего доступа к файлу)	Если на сервере хранятся файлы, доступ к которым открыт только на чтение, то, отметив этот флажок, можно существенно повысить производительность системы.
FTP Logon	Регистрация по FTP
Allow anonymous FTP logon (разрешить анонимную регистрацию по FTP)	Разрешает анонимным пользователям регистрироваться по FTP. В системах с повышенной защитой этот флажок надо сбросить. Если отмечен дополнительно флажок Allow only anonymous FTP logon , то по FTP будут возможны только анонимные регистрации. При этом можно указать имя анонимного пользователя в поле Anonymous FTP logon alias .
Specify home directory (Указать домашний каталог)	Указывается каталог, в который попадает каждый новый пользователь после регистрации.
Log successful anonymous logon (Фиксировать успешную анонимную регистрацию)	Можно вести учет всех пользователей, зарегистрировавшихся по FTP. Необходимо указать каталог, в котором находится файл регистрации пользователей.
Connection timeout (Тайм-аут при соединении)	Указывается промежуток времени, по истечении которого пользователь будет отключен от FTP-сервера в случае отсутствия какой-либо деятельности.

Параметры принтеров Windows NT (Windows NT Printers)

Параметр	Описание
Disable browse thread on this computer (Запретить просмотр на этом компьютере)	Когда отмечен этот флажок, спулер печати не посылает информацию о принтере на другие серверы печати.
Scheduler priority (приоритет планировщика)	Устанавливается приоритет планировщика печати. Доступны три значения: Above normal (выше нормального) Normal (нормальный) Below normal (ниже нормального)
Beep for error enabled (Сигнал в случае ошибки)	Если отмечен этот флажок, то в случае ошибки на удаленном сервере печати каждые 10 секунд раздается звуковой сигнал.

Параметры удаленного доступа Windows NT (Windows NT Remote Access)

Параметр	Описание
Max number of unsuccessful authentication retries (Максимальное число неудачных попыток аутентификации)	Указывается максимально допустимое число попыток аутентификации удаленного пользователя. При превышении происходит разрыв связи. По умолчанию — 2.
Max time limit for authentication (Максимальное время аутентификации)	Указывается максимальное время, отводимое на аутентификацию. При превышении происходит разрыв связи. По умолчанию 120 секунд.
Wait interval for callback (Время ожидания обратной связи)	Указывается интервал времени, в течение которого ожидается звонок для установления обратной связи. По истечении этого промежутка система переходит в исходное состояние.
Auto disconnect (Автоматическое отключение)	Если в течение указанного интервала времени не наблюдалась активность по каналу удаленного доступа, происходит автоматический обрыв связи. По умолчанию 20 минут. Однако следует помнить, что на сервере этот интервал может быть меньше.

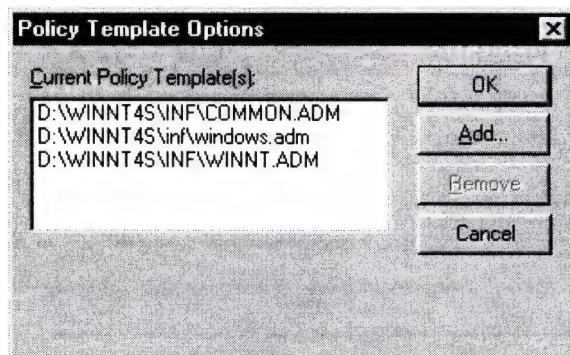
Параметры профилей пользователей Windows NT (Windows NT Users Profiles)

Параметр	Описание
Automatically detect slow network connections (автоматически определять медленные каналы)	Автоматически определяется работа по медленному каналу связи. В этом случае не передается информация обо всех профилях.
Slow network connection timeout (тайм-аут для медленного канала)	Если в течение указанного интервала времени не наблюдалась активность по медленному каналу, выдается сообщение о тайм-ауте
Timeout for dialog boxes (тайм-аут для диалоговых окон)	Время неактивности диалоговых окон.

Шаблоны для формирования системной политики

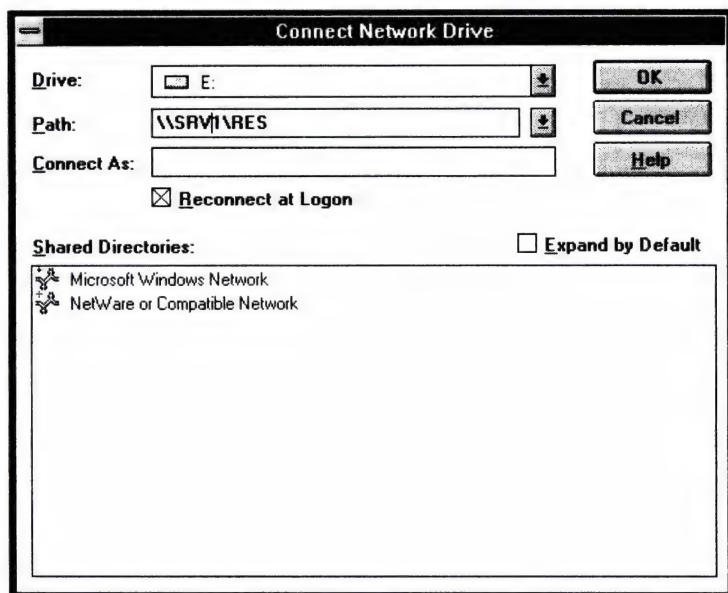
Редактор системной политики, как мы уже говорили, использует шаблоны, т.е. текстовые файлы с расширением .ADM, хранящиеся в каталоге **%systemroot%\INF**. Вы можете создавать свои собственные шаблоны для настройки приложений, используемых в корпоративной среде. Например, внутрифирменные базы данных, система электронной почты, оперенд и др. Понятно, что эти приложения должны хранить свои настройки в реестре, а не в INI-файлах.

Для загрузки нового шаблона в редактор системной политики убедитесь, что текущий файл закрыт (изображается равномерное серое поле), и в меню **Options** выберите команду **Policy Template**. В появившемся диалоговом окне нажмите кнопку **Add** и укажите новый (или дополнительный) файл-шаблон.



Диалоговое окно *Policy Template Options*.

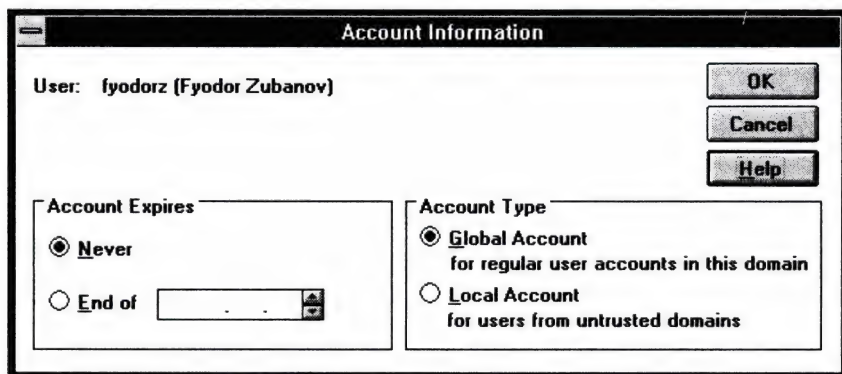
Что реально происходит при добавлении нового шаблона? Каждый шаблон содержит набор ключей реестра в различных его ветвях. Поэтому добавление нового шаблона выразится в появлении новых значений, доступных для редактирования редактором системной политики и соответствующих иным ветвям и ключам реестра. На рисунке схематично показано образование нового файла системной политики при слиянии шаблонов.



В шаблонах применяется несколько ключевых слов, синтаксических конструкций и символов. Подробнее о структуре шаблона см. книгу *Ресурсы Windows 95*.

Определение общих параметров учетной записи

Чтобы определить общие параметры учетной записи — срок ее действия и принадлежность к локальным или глобальным — “нажмите” кнопку **Account** в диалоговом окне **Users Properties**.



Диалоговое окно *Account Information*.

В появившемся диалоговом окне укажите срок действия учетной записи. По умолчанию учетная запись не имеет ограничений по времени. Но если Вы, например, наняли временного сотрудника, установите срок жизни учетной записи равным сроку его работы в организации. Это гарантия от случайного или преднамеренного доступа данного сотрудника в сеть по истечении срока контракта.

По умолчанию вновь создаваемая учетная запись является глобальной и принадлежит домену. Если же надо сделать учетную запись локальной для данного сервера, пометьте соответствующий флажок. О назначении и различиях глобальных и локальных учетных записей см. раздел *Учетные записи пользователей*.

Управление политикой ведения учетных записей

Рассматривая выше средства администрирования индивидуальных пользователей, мы показали возможность определения правил изменения пароля и привилегий для каждого пользователя. Но существует ряд общих для сервера или домена в целом параметров, позволяющих заметно повысить защищенность. Эти параметры объединены в одно общее понятие: *политика ведения учетных записей*. Для управления политикой ведения учетных записей в Windows NT версии 3.5х используется **User Manager for Domains** (на сервере) и **User Manager** (на рабочей станции), а в Windows NT версии 4.0 добавляется и рассмотренный ранее редактор системной политики **System Policy Editor**.

Account Policy

Domain: **MOW-DEMO-M**

Password Restrictions

Maximum Password Age <input type="radio"/> Password <u>N</u> ever Expires <input checked="" type="radio"/> Expires In 42 Days	Minimum Password Age <input checked="" type="radio"/> Allow Changes Immediately <input type="radio"/> Allow Changes In Days
Minimum Password Length <input checked="" type="radio"/> Permit <u>B</u> lank Password <input type="radio"/> At Least Characters	Password Uniqueness <input checked="" type="radio"/> Do Not Keep Password History <input type="radio"/> Remember Passwords

☒ No account lockout
☐ Account lockout

Lockout after bad logon attempts
 Reset count after minutes
 Lockout Duration
☐ Forever (until admin unlocks)
☐ Duration minutes

☐ Forcibly disconnect remote users from server when logon hours expire
☐ Users must log on in order to change password

OK Cancel Help

Политикой задаются:

- максимальный срок действия пароля;
- минимальная длина пароля;
- минимальный срок сохранения пароля неизменным;
- уникальность пароля;
- блокировка учетных записей при неудачной регистрации;
- продолжительность блокировки;

а также некоторые другие параметры.

Установка максимального срока действия пароля

Если пользователь долго не меняет своего пароля, защищенность системы от несанкционированного доступа, безусловно, снижается. Случается, во время регистрации в системе некто посторонний подсматривает за вводимым паролем, а потом пользуется им. А кое-кто для простоты набирает стандартные комбинации вроде даты рождения, своего имени или имен ближайших родственников, названия компьютера, за которым работает и т.п. Вероятность раскрытия такого пароля, естественно, высока. Поэтому-то система должна принуждать пользователя к периодической смене пароля.

Политика ведения учетных записей позволяет установить определенный срок действия пароля в пределах от 1 до 999 дней или сделать его постоянным. По умолчанию предлагается установить продолжительность действия пароля в 42 дня. Если же Вы предъявляете повышенные требования к защищенности сети, то рекомендуемое значение — менее 30 дней.

Когда приблизится конец срока действия пароля, пользователю при регистрации в системе будет выдано сообщение о том, что срок действия пароля кончается через N дней, и предложено изменить пароль незамедлительно. Пока срок действия пароля не истек, данное сообщение можно игнорировать или изменить пароль. Если же пароль так и не будет изменен, учетная запись будет заблокирована.

Если администратор указал опцию ***Password Never Expires*** для конкретного пользователя, последний может не менять пароль. Это рекомендуется делать только для служебных учетных записей, от имени которых исполняются сервисы в системе.

Изменение минимальной длины пароля

По умолчанию длина пароля, устанавливаемого пользователем, варьируется от 0 до 14 символов. Понятно, что при повышенных требованиях к защищенности системы пустой пароль недопустим. В этом случае администратор системы должен определить в политике ведения учетных записей минимальную длину пароля. Рекомендуемый минимум — 6 символов.

Создавая новую учетную запись для пользователя, администратор может указать пароль произвольной длины независимо от ограничения, заданного политикой ведения учетных записей. Но если пользователь будет изменять свой пароль после регистрации в системе, он сможет ввести пароль только в соответствии с политикой ведения учетных записей.

Описанная ситуация таит в себе опасность. Допустим, администратор назначил новому пользователю пустой пароль и установил флажок ***User Must Change Password At Next Logon***. Естественно, регистрируясь в первый раз, пользователь заменит пароль на новый в соответствии с установленной политикой ведения учетных записей. Но пока пользователь не выполнит эту первую регистрацию, пароль по-прежнему останется пустым. Поэтому, создавая новую учетную запись, администратор должен назначать пароль длиной минимум 6 символов, что в большинстве случаев достаточно надежно.

Установка продолжительности запрета на изменение пароля пользователем

В ряде случаев применяется параметр, ограничивающий минимальное время, через которое пользователь может изменять свой пароль.

Во-первых, если в системе работает много пользователей, недавно познакомившихся с системой Windows NT, имеет смысл установить определенный срок, в течение которого они привыкнут к особенностям защищенной работы и поймут необходимость запоминания своего пароля. Тогда новичок, даже забыв свой пароль, на первых порах сможет обратиться к администратору, чтобы тот напомнил комбинацию, установленную некоторое время назад.

Во-вторых, новичок, сменив по истечении срока действия пароль, может захотеть вернуться к прежнему. Так как это ослабит защищенность системы, принудительная задержка не позволит это сделать. Это особенно эффективно, если установить параметр отслеживания уникальности пароля, описанный ниже.

Минимальный период для разрешения смены пароля по умолчанию не ограничивается и варьируется в пределах от 1 до 999 дней. Обычно достаточно 14 дней.

Если для конкретного пользователя администратор указал *Allow Changes Immediately*, последний может изменять пароль в любое время.

Хранение истории паролей

Данный параметр позволяет запоминать в системе от 1 до 24 паролей, что обеспечивает на протяжении длительного времени уникальные пароли для пользователя. Данный параметр особенно эффективен совместно с ограничением периода, в течение которого пользователю запрещено изменять пароль. Допустим, Вы установили 10 дней, указав необходимость сохранения 20 паролей. Тогда пользователь, сменив пароль, сможет его применять снова только через 200 дней.

Блокировка учетных записей

Следующая группа параметров связана с защитой системы от незаконного проникновения путем подбора пароля. Предположим, злоумышленнику известно имя учетной записи пользователя. Тогда он может подобрать пароль либо вручную, либо с помощью специальной программы. Чтобы этого не случилось, установите максимальное число неудачных попыток регистрации (по умолчанию 5), после которых учетная запись будет заблокирована. Еще можно указать время, через которое счет неудачных попыток сбросится (по умолчанию 20 минут), и время, в течение которого учетная запись будет заблокирована (по умолчанию 1 час). После удачной регистрации счет неудачных регистраций будет обнулен.

Устанавливаемые периоды блокировки зависят от условий работы. Обычно устанавливаемых по умолчанию значений вполне достаточно. Не рекомендуется устанавливать “вечную” продолжительность блокировки (т.е. до разблокирования его администратором). Эта установка таит потенциальную опасность. Зная имена учетных записей всех администраторов системы, злоумышленник без труда заблокирует их, и система станет неуправляемой. Поэтому устанавливайте длительный, но разумный промежуток времени.

Сказанное не относится к учетной записи **Administrator** — она не блокируется. Но при этом можно использовать неограниченное число попыток подбора пароля. Выход из этой ситуации — дать учетной записи **Administrator** какое-либо еще, известное только администратору системы имя.

Принудительное отключение удаленных пользователей по истечении разрешенного времени работы

Эта функция позволяет системе отключать пользователей, чье установленное допустимое время работы истекло. По умолчанию система их не отключает, но если эта опция установлена, то за несколько минут до истечения указанного времени система предупредит пользователя о предстоящем отключении и точно в срок выполнит отключение. Если же этот флажок не помечен, система будет предупреждать пользователя об истекшем времени работы каждые 10 минут. Новая регистрация в системе после истечения срока невозможна.

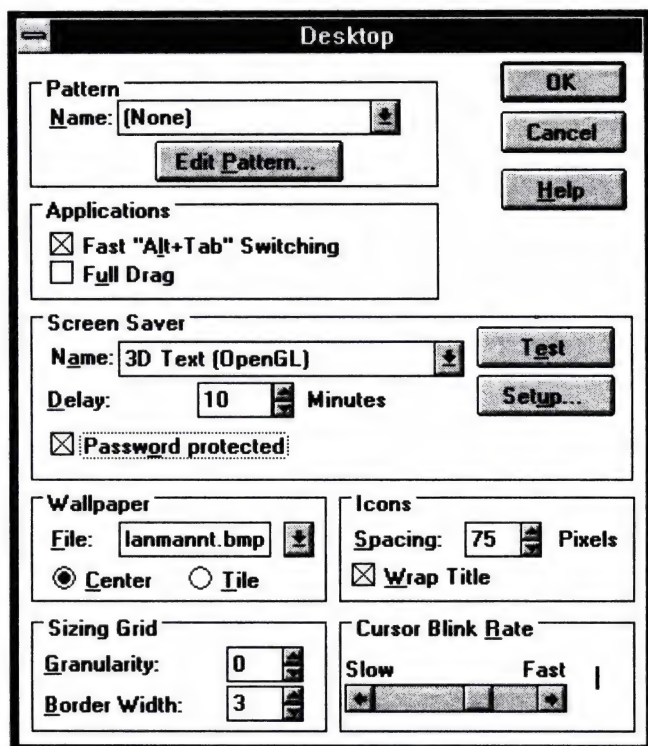
Если пользователь инициировал некоторый процесс, окончание которого выходит за разрешенные временные рамки, этот процесс будет принудительно прерван. Единственный выход — попросить администратора дать дополнительное время.

Обязательность регистрации для смены пароля

Если помечена соответствующая опция, пользователь, прежде чем изменить свой пароль, должен зарегистрироваться в системе. Иначе он сделает это и без регистрации. Это особенно актуально, когда истекает срок действия пароля. Если опция помечена, пользователь самостоятельно не изменит пароль, и ему придется обратиться к администратору. Если нет, пароль можно изменить, не ставя администратора в известность.

Блокировка рабочей станции

С помощью этой функции можно автоматически блокировать рабочую станцию через определенный период, в течение которого не было активности со стороны клавиатуры или мыши. Это обеспечивает защиту от несанкционированного доступа к компьютеру в период временного отсутствия пользователя на рабочем месте. Данная функция, совмещенная с заставками экрана, доступна через настройку параметров **Desktop** в **Control Panel** (по умолчанию не отмечена).



Установка параметров блокировки рабочей станции в параметрах Заставок экрана (Screen Saver).

Время задержки блокировки устанавливайте осмотрительно. У пользователя может сложиться ложное ощущение безопасности, когда он отходит от своего рабочего места. Но он забывает, что, пока рабочая станция будет заблокирована, пройдет какое-то время. Очень маленький промежуток времени сделает работу не совсем удобной, так как даже небольшие паузы в работе вызовут блокировку консоли. Поэтому блокируйте консоль принудительно перед тем, как покинуть рабочее место.

Файловая система NTFS

С момента появления самой первой бета-версии Windows NT в 1992 году разгорелись споры об используемой в ней файловой системе NTFS. То, что ее структура долгое время оставалась неопи­санный в печати, поро­ждало массу домыслов о ее достоинствах и недостатках. Даже сей­час не всем ясно, за счет чего достигнута столь высокая надежность и способность этой системы к быстрому самовосстановлению в случае краха. Добавьте еще способность контролировать доступ к каждому файлу, поддержку огромных дисков (до 408 млн Тбайт), UNICODE и ряд других функций, и Вы получите уникальную в своем роде систему.



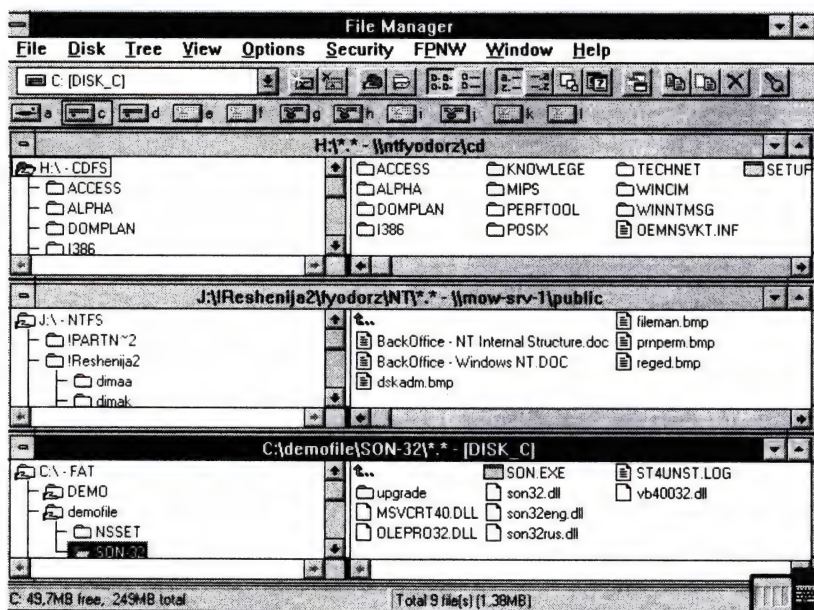
Файловые системы Windows NT

В Windows NT поддерживаются четыре файловые системы:

- Windows NT file system (NTFS) — исключительно для Windows NT;
- File Allocation Table (FAT) — для совместимости с приложениями MS-DOS;
- High Performance File System (HPFS) — для совместимости с приложениями OS/2;
- CD-ROM File System (CDFS) (так как эта файловая система не позволяет записывать информацию, я ее не рассматриваю).

Выбор системы зависит от предъявляемых к ней требований и используемых приложений. У каждой свои полезные свойства, но возможности защиты и аудита систем различны.

Windows NT может поддерживать Named Pipes File System (NPFS) и Mailslot File System (MSFS), используемые для связи между процессами (в книге они не рассматриваются).



Изображение дисков с различными файловыми системами в окне File Manager.

Файловая система FAT

Файловая система FAT (File Allocation Table) получила свое наименование названию метода организации данных — таблицы распределения файлов. FAT первоначально была ориентирована на небольшие диски и простые структуры каталога. Через несколько лет ее усовершенствовали для обеспечения возможности работы с большими дисками и мощными персональными компьютерами.

На рисунке показана организация диска с использованием FAT:

Блок параметров BIOS	FAT1	FAT2 (копия)	Корневой каталог	Область файлов...
----------------------	------	--------------	------------------	-------------------

Дисковый раздел FAT.

Windows NT версии 3.5 и выше использует биты атрибута для поддержки длинных имен файлов (до 255 символов) в разделах FAT. Применяемый для этого способ не мешает MS-DOS или OS/2 обращаться к подобному разделу. Всякий раз при создании пользователем файла с длинным именем (превышающим стандартное для FAT ограничение “8+3”) Windows NT создает элемент каталога для этого файла, соответствующий соглашению “8+3”, по тем правилам, что и для NTFS, плюс один или несколько вторичных элементов каталога. Каждый из этих вторичных элементов рассчитан на 13 символов в длинном имени файла. Вторичные элементы сохраняют длинную часть имени файла в UNICODE. Для этих элементов устанавливаются атрибуты: том, системный, скрытый, только для чтения. MS-DOS и OS/2 игнорируют элементы каталога с таким набором атрибутов, поэтому они невидимы в этих операционных системах. Вместо них MS-DOS и OS/2 обращаются к стандартным элементам, содержащим информацию в стандарте “8+3”.

Некоторые дисковые утилиты сторонних производителей, взаимодействующие непосредственно с FAT, могут расценивать созданные Windows NT элементы каталога с длинным именем файла как ошибки логической структуры тома. Попытки этих утилит исправить ошибки могут привести к потере файлов и каталогов. Не используйте утилиты работы с диском или дефрагментирования диска, не проверенные на совместимость с Windows NT.

Файловая система Windows NT FAT функционирует аналогично MS-DOS и Windows. Windows NT можно устанавливать на существующем разделе FAT. Если же компьютер работает под управлением Windows 95, можно свободно создавать длинные имена файлов и каталогов, так как механизмы работы с длинными именами в обеих системах одинаковы.

Нельзя использовать Windows NT с любыми программами сжатия или разбиения диска на разделы, если программное обеспечение требует драйверов MS-DOS. Для чтения подобных дисков нужны драйверы Windows NT.

FAT — система с точной записью. Это означает, что при необходимости изменения структуры тома дается команда записи на диск. Недостаток такой системы — медленное выполнение преобразованных в последовательность операций записи. Дело в том, что первая запись на диск должна быть завершена прежде, чем начнется вторая и т.д. Это не самое эффективное использование возможностей мощных компьютеров.

Допускается безболезненный перенос или копирование файлов с тома FAT на NTFS. При выполнении обратной операции информация о разрешениях и альтернативных потоках будет потеряна.



Внимание: FAT не обеспечивает функций защиты данных и автоматического восстановления. Поэтому она используется, только если альтернативной системой на компьютере является MS-DOS или Windows 95, а также для передачи данных на гибких дисках. Кроме того, для RISC-систем необходимо, чтобы небольшой загрузочный раздел был отформатирован под FAT. В остальных случаях использовать FAT не рекомендуется.

Файловая система HPFS

HPFS имеет особенности, способствующие эффективному управлению большими объемами жесткого диска. HPFS поддерживает длинные (до 255 символов) имена файлов.

Когда том форматируется под HPFS, первые 18 секторов резервируются для блока начальной загрузки, суперблока и запасного блока. Эти структуры используются для загрузки операционной системы, поддержки файловой системы и восстановления при возможных ошибках.

В HPFS резервируется пространство под два битовых массива объемом 2 Кб для каждого дискового интервала в 16 Мб. Каждый массив отводит по одному биту для каждого размещаемого блока (равного одному сектору) в полосе 8 Мб, показывая, какие размещаемые блоки используются.

Битовые массивы поочередно размещаются в конце и начале каждой полосы, обеспечивая таким образом максимальное количество непрерывного пространства для данных (16 Мб). Кроме того, запись новых файлов планируется так, что между новым и существующим файлами остается свободный участок, чтобы каждый файл имел возможность расширения в непрерыв-

ном дисковом пространстве. Это свойство HPFS помогает осуществлять быстрый поиск данных и минимизировать фрагментацию файлов.

Другая особенность, объясняющая быстрый поиск в каталоге, — технология B-tree. Эта древовидная структура с корнем и несколькими узлами содержит данные, организованные некоторым логическим способом. Корень содержит административную информацию, карту для остальной структуры и, возможно, некоторые данные. Большинство данных содержится в узлах. С большими каталогами технология B-tree работает гораздо эффективнее линейных списков, используемых FAT.


HPFS применяет B-tree для структуризации каждого файла и каталога. Каждый каталог указывает на структуры Fnode для содержащихся в нем файлов. Структура Fnode (ее размер 512 байтов) содержит заголовок, имя файла (усеченное до 15 символов), длину файла, расширенные атрибуты, список контроля доступа (ACL) и расположение данных файла.

ACL HPFS поддерживаются только операционной системой OS/2, но не Windows NT. Для использования списков контроля доступа необходима NTFS.

HPFS эффективно работает на дисках объемом до 2 Гб. Однако есть у нее и слабые стороны. Например, если повреждена первая часть тома с информацией начальной загрузки и указателем на корневой каталог, том использовать невозможно. Применение утилиты **chkdsk** при каждой начальной загрузке системы и восстановление диска после ошибки требует длительного времени. Кроме того, HPFS предполагает применение 512-байтовых секторов, которые не очень годятся для больших томов.

HPFS — система с отложенной записью. Работа с данными производится через буфер ввода/вывода. Пока пользователь читает файлы или просматривает каталоги, необходимые для записи, данные накапливаются в кэше. Так что ждать окончания процесса записи не нужно. Запись данных на диск производится только в момент низкой загрузки ресурсов компьютера. Недостаток систем с отложенной записью в том, что в случае сбоя диска восстановление данных займет гораздо больше времени, чем в системе с точной записью. Это происходит из-за того, что утилита **chkdsk** должна просканировать весь том для проверки его фактического состояния.

Windows NT поддерживает HPFS прежде всего для совместимости снизу вверх при выборочной загрузке OS/2 или Windows NT. Если использование OS/2 не планируется, применять HPFS не рекомендуется.



Замечание: В Windows NT версии 4.0 файловая система HPFS больше не поддерживается.

Файловая система NTFS

NTFS обеспечивает сочетание эффективности, надежности и совместимости, невозможное в FAT или HPFS. Она разработана для быстрого выполнения стандартных файловых операций вроде чтения, записи и поиска, а также улучшенных операций, например восстановления файловой системы на очень больших жестких дисках.

NTFS, включая возможности безопасности, требуемые для файловых серверов и высококачественных персональных компьютеров в корпоративной среде, поддерживает управление доступом к данным и привилегии владельца, что важно для целостности корпоративных данных.

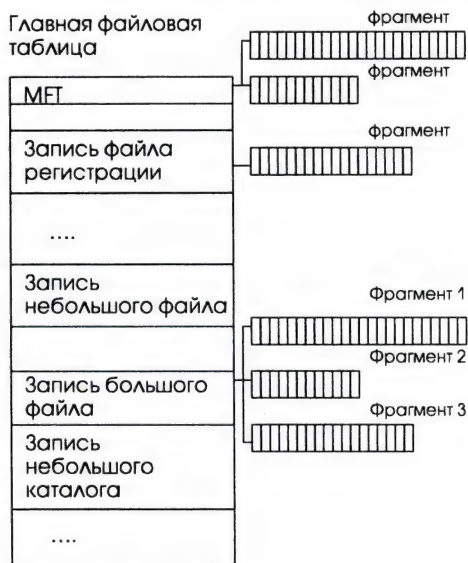
NTFS — простая, но очень мощная разработка, для которой вся информация на томе NTFS — файл или часть файла. Каждый распределенный на томе NTFS сектор принадлежит некоторому файлу. Частью файла являются даже метаданные файловой системы (информация, описывающая непосредственно файловую систему).

Эта основанная на атрибутах файловая система поддерживает объектно-ориентированные приложения, обрабатывая все файлы как объекты с атрибутами, определяемыми пользователем и системой.

Главная файловая таблица

Каждый файл на томе NTFS представлен записью в специальном файле — главной файловой таблице (Master File Table — MFT). NTFS резервирует первые 16 записей таблицы для специальной информации. Первая запись таблицы описывает непосредственно главную файловую таблицу. За ней следует зеркальная запись MFT. Если первая запись MFT разрушена, NTFS читает вторую запись для отыскания зеркального файла MFT, первая запись которого идентична первой записи MFT. Местоположения сегментов данных MFT и зеркального файла MFT записаны в секторе начальной загрузки. Дубликат сектора начальной загрузки находится в логическом центре диска.

Третья запись MFT — файл регистрации, применяемый для восстановления файлов. Семнадцатая и последующие записи главной файловой таблицы используются собственно файлами и каталогами на томе. На рисунке показана упрощенная структура MFT, обеспечивающая очень быстрый доступ к файлам.



Организация главной файловой таблицы.

Целостность данных и восстановление в NTFS

NTFS — это восстанавливаемая файловая система, сочетающаяся быстродействие файловой системы с отложенной записью и практически мгновенное восстановление.

Каждая операция ввода/вывода, изменяющая файл на томе NTFS, рассматривается файловой системой как транзакция и может выполняться как неделимый блок. При модификации файла пользователем сервис файла регистрации фиксирует всю информацию, необходимую для повторения или отката транзакции. Если транзакция завершена успешно, производится модификация файла. Если нет, NTFS производит откат транзакции, следуя инструкциям в информации отмены. При обнаружении в транзакции ошибки транзакция прокручивается обратно.

Файловая система восстанавливается очень просто. При сбое системы NTFS выполняет три прохода: анализа, повторов и откатов. В течение анализа на основании информации файла регистрации NTFS оценивает повреждение и точно определяет, какие кластеры нужно модифицировать. При повторном проходе выполняются все этапы транзакции от последней контрольной точки. Откат осуществляет возврат всех незавершенных транзакций.

Важная особенность NTFS — отложенная передача (lazy commit) — позволяет минимизировать затраты на регистрацию транзакций и подобна отложенной записи. Вместо использования ресурсов для немедленной отметки транзакции как успешно завершенной эта информация заносится в кэш и записывается в файл регистрации как фоновый процесс. Если сбой происходит до того, как информация о транзакции была зарегистрирована, NTFS произведет повторную проверку транзакции для определения ее успешности. Если NTFS не может гарантировать, что транзакция завершилась успешно, производится откат транзакции. Никакие незавершенные модификации тома не разрешены.

Каждые несколько секунд NTFS проверяет кэш, чтобы определить состояние отложенной записи и отметить его в файле регистрации как контрольную точку. Если после определения контрольной точки произойдет сбой, система имеет возможность привести свое состояние к зафиксированному контрольной точкой. Данный метод использует оптимальное время восстановления, сохраняя очередь событий, которая может потребоваться в процессе восстановления. Этот уровень предназначен для защиты метаданных — пользовательские в случае сбоя системы могут быть разрушены.

Объем журнала транзакций устанавливается командой **CHKDSK /L:размер**. Размер указывается в килобайтах. По умолчанию он равен 4 096 Кб. Чтобы узнать текущий размер журнала, выполните команду **chkdsk /L**.

Длинные и короткие имена файлов

NTFS поддерживает длинные имена файлов (до 255 символов). В имени файла используются символы UNICODE, что позволяет создавать файлы, содержащие, например, символы кириллицы. При этом автоматически решен вопрос доступа из MS-DOS приложений. NTFS автоматически генерирует стандартное для MS-DOS имя вида "8+3".

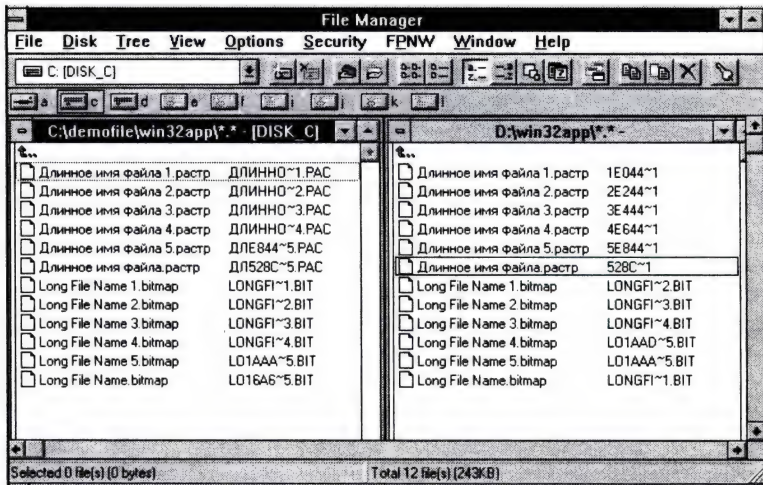
Набор символов UNICODE для имен файлов делает возможным применение "запрещенных" символов, которые MS-DOS- и Windows-приложения не читают. Поэтому при генерации короткого имени удаляются все такие символы и любые пробелы. Далее при необходимости имя усекается до 6 символов и добавляется тильда (~) с последующим номером. Повторяющиеся имена файлов заканчиваются символами 2, 3 и т. д. Расширение имени файла усекается до трех символов. В Windows NT 3.5x используется несколько иной алгоритм при числе файлов с одинаковым началом больше 5. Для пятого и последующих файлов Windows NT использует только два первых символа и далее специальной математической операцией генерирует четыре уникальных символа. Последними двумя символами в файле являются ~5. Этот метод применяется для томов FAT и NTFS. Ниже приведены примеры таких имен файлов. Однако при использовании полностью русских имен файлов указанный порядок преобразования соблюдается только на томах FAT. На томах NTFS формируется новое короткое имя файла примерно так,

как показано на рисунке. Если в русском имени файла есть хотя бы одно английское слово, оно будет взято за основу короткого имени, если нет — короткое имя будет сформировано на основе составляющих имя кодов UNICODE.

40

В Windows NT версии 4.0 можно указать в реестре допустимость использования расширенных (читай национальных) символов в коротких именах файлов. Для этого можно воспользоваться либо редактором системной политики (*System policy editor*), либо ввести новое значение непосредственно. При этом следует помнить, что для клиентов, на которых не установлена соответствующая кодовая страница такие файлы будут недоступны. Так, например, если у Вас имеются MS-DOS клиенты, на которых используется русификатор, не устанавливающий 866 кодовую страницу, они не увидят правильных русских имен файлов на сервере и не смогут их открыть.

Ветвь: HKEY_LOCAL_MACHINE
Ключ: SYSTEM\CurrentControlSet\Control\FileSystem
Имя: NtfsAllowExtendedCharacterIn8Dot3Name
Значение: 1
Тип: DWORD



Преобразование длинных имен файлов в короткие на FAT (слева) и NTFS.

Длинное имя файла теряется при сохранении приложениями MS-DOS или Windows 3.x на том NTFS, если приложение сохраняет временный файл, удаляет первоначальный файл и переименовывает временный файл в файл с первоначальным именем. Теряется и любой уникальный набор расширений файла. Права передаются заново из родительского каталога.



Внимание: В версии Windows NT Server 3.51 есть ошибка, связанная с созданием и модификацией длинных русских имен файлов и каталогов. При попытке модификации или удаления такого файла с рабочей станции (неважно, какой именно — Windows NT Workstation 3.51 или Windows 95) файл не удаляется, а переносится в корневой каталог с потерей первой буквы в названии и преобразованием всех букв в имени в буквы верхнего регистра! Поэтому настоятельно не советую создавать файлы и каталоги с длинными русскими именами. Эта ошибка исправлена только в версии 4.0.

Компрессия файлов и каталогов

Особенностью NTFS является возможность динамического сжатия файлов и каталогов. Тот, кто работал с MS-DOS наверняка использовал утилиты динамического сжатия дисков Drivespace или Stack. Грубо говоря, компрессия на NTFS предлагает то же самое. Однако в отличие от упомянутых утилит в Windows NT компрессия возможна как для отдельных каталогов, так и файлов на диске. Сжатие является новым атрибутом файла или каталога, и, подобно любому атрибуту, он может быть снят или установлен в любой момент времени.



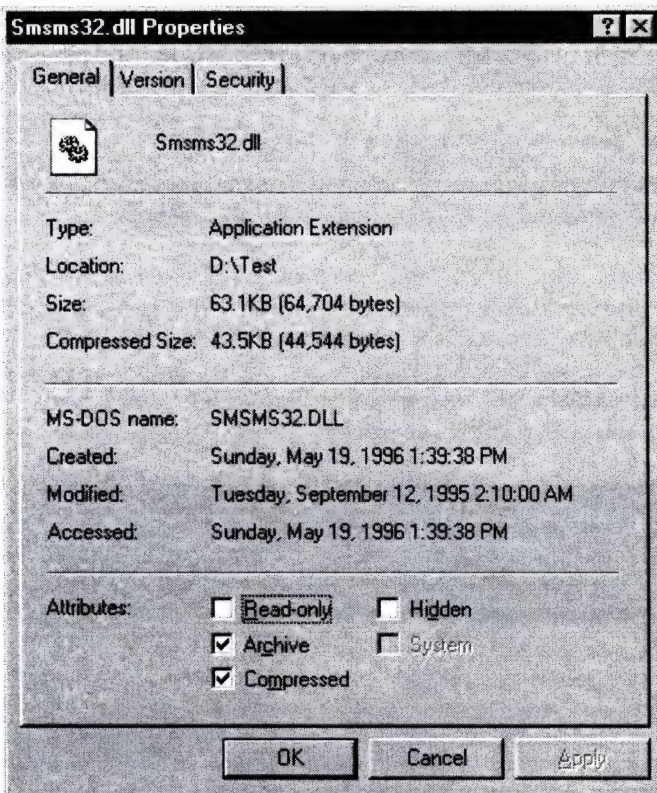
Замечание: Сжатие возможно только на разделах, размер блока которых не превышает 4 096 байтов. Для установки размера блока используется команда **FORMAT /A:размер**.

Если каталог имеет атрибут **Compressed**, то все файлы, копируемые в этот каталог, также получают этот атрибут. Чтобы вновь создаваемый раздел диска автоматически сжимал все создаваемые и копируемые файлы, его надо отформатировать с ключом /C, т.е. **FORMAT диск: /C /FS:NTFS**.

Для сжатия существующего файла или каталога используется либо команда **Compress**, либо **Properties** в **File Manager**. Все сжатые файлы и каталоги отображаются в **File Manager** синим цветом.

4.0

В Windows NT 4.0 атрибуты файлов назначаются либо через **File Manager**, либо через **Explorer** вызовом диалогового окна **File Properties**.



Диалоговое окно **File Properties**.

По умолчанию сжатые файлы не выделяются при просмотре папок другим цветом. Если Вы хотите видеть эту разницу, отметьте соответствующий флажок в окне настроек **View Options**.

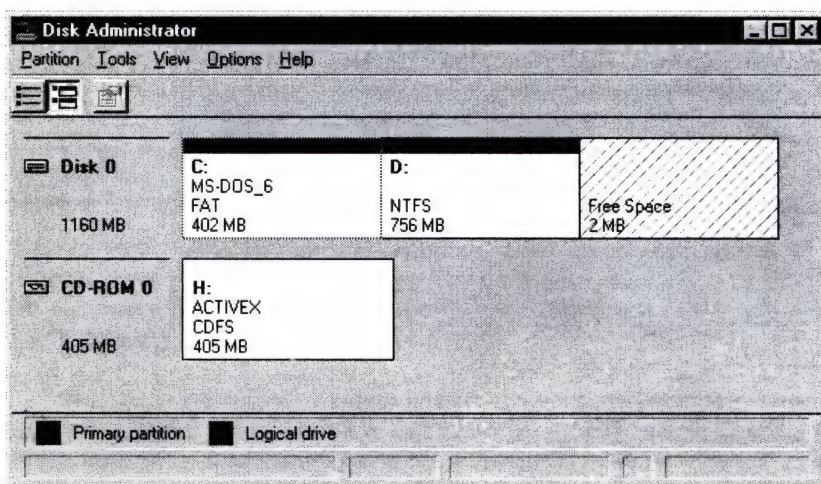
Степень сжатия файлов зависит от типа файла. Наиболее эффективно применять этот атрибут к файлам документов Microsoft Word, PowerPoint, графическим файлам и т.п. Организуя файл-сервер, имеет смысл сжать все персональные каталоги пользователей. С другой стороны, совершенно неэффективно сжимать каталоги, содержащие дистрибутивы программных продуктов. Это не даст абсолютно никакого выигрыша, так как они, как правило, достаточно сжаты.

Создание и модификация разделов диска

Работая с другими операционными системами (например MS-DOS или Windows 95), Вы использовали программу FDISK для модификации разделов диска и команду FORMAT для их форматирования. Начиная работать в Windows NT, Вы, естественно, твердо убеждены в том, что:

- а) эти команды должны существовать в Windows NT;
- б) изменение формата раздела диска возможно только командой FORMAT с полной потерей данных находящихся на формируемом диске.

Первая же попытка запустить FDISK заканчивается неудачей: подобной утилиты не существует. Особо пытливые загружают с дискеты MS-DOS и запускают эту утилиту из него. К их удивлению, NTFS-разделы не поддаются уничтожению! Что делать? Ответ один — запустить административную программу **Disk Administrator**, имеющую графический интерфейс и позволяющую манипулировать разделами диска.



Окно программы Disk Administrator.

С помощью администратора дисков можно не только изменить разбиение физического диска на разделы, но и изменить их формат, присвоить иную букву для диска, объединять несколько разделов в один логический том, а также использовать механизмы повышенной надежности работы с диском, описанные в главе *Обеспечение отказоустойчивости*.

В отличие от команды FDISK команда FORMAT по-прежнему присутствует в системе, но содержит ряд дополнительных ключей:

```
FORMAT drive: [/V:label] [/Q] [/T:tracks /N:sectors]
```

```
FORMAT drive: [/V:label] [/Q] [/1] [/4]
```

```
FORMAT drive: [/Q] [/1] [/4] [/8]
```

```

    /FS:file-system Specifies the type of the file system (FAT or NTFS).
    /V:label         Specifies the volume label.
    /Q              Performs a quick format.
    /C              Files created on the new volume will be compressed by
                    default.
    /A:size          Overrides the default allocation unit size. Default
settings are strongly recommended for general use.
                    NTFS supports 512, 1024, 2048, 4096, 8192, 16K, 32K, 64K.
                    FAT supports 8192, 16K, 32K, 64K, 128K, 256K.
                    NTFS compression is not supported for allocation unit
sizes above 4096.
    /F:size          Specifies the size of the floppy disk to format (160,
                    180, 320, 360, 720, 1.2, 1.44, 2.88, or 20.8).
    /T:tracks        Specifies the number of tracks per disk side.
    /N:sectors        Specifies the number of sectors per track.
    /1               Formats a single side of a floppy disk.
    /4               Formats a 5.25-inch 360K floppy disk in a
                    high-density drive.
    /8               Formats eight sectors per track.

```

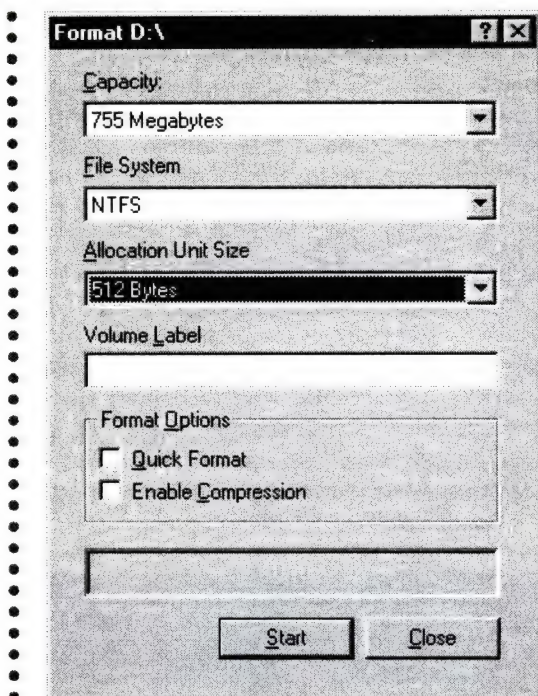
Так, в частности, можно форматировать дискеты объемом до 20,8 Мбайт, указывать тип файловой системы, размер блока на диске, что важно с точки зрения оптимизации производительности файл-сервера.

Команда **FORMAT** — самое универсальное средство форматирования — доступна всегда. Если выбранный для форматирования диск не может быть отформатирован в данный момент по какой-либо причине, эта операция будет перенесена на момент перезагрузки системы.

Как уже говорилось, для форматирования дисков можно также использовать и администратор дисков, а для форматирования дискет — **File Manager**.

- В Windows NT 4.0 щелчок правой кнопкой мыши названия диска в **Windows NT Explorer** с последующим выбором в меню команды **Format** приводит к запуску графической программы форматирования дисков, более удобной для начинающих администраторов.





Графическая программа форматирования.

Преобразование существующего раздела в формат NTFS

Случается, что спустя некоторое время после установки сервера, его полной конфигурации и введения в рабочий режим администратор спохватывается и решает преобразовать формат диска, на котором располагаются каталоги пользователей (или иные важные данные) в NTFS для обеспечения более высокой степени защиты. К сожалению незнание того, что в системе существует команда **CONVERT**, вынуждает его долго тянуть с этим мероприятием, так как он уверен, что без потери данных или выполнения полного резервного копирования с последующим восстановлением здесь не обойтись.

Но стоит только запустить команду **CONVERT**, чтобы узнать, что она позволяет преобразовать разделы FAT или HPFS в раздел NTFS без потери данных!

CONVERT drive: /FS:NTFS [/V]

drive	Specifies the drive to convert to NTFS. Note that you cannot convert the current drive.
/FS:NTFS	Specifies to convert the volume to NTFS.
/V	Specifies that Convert should be run in verbose mode.

Главное помните о невозможности преобразования активного раздела. В этом случае система может отсрочить выполнение преобразования до следующей перезагрузки операционной системы.

Права на доступ к файлам и каталогам. Понятие владельца

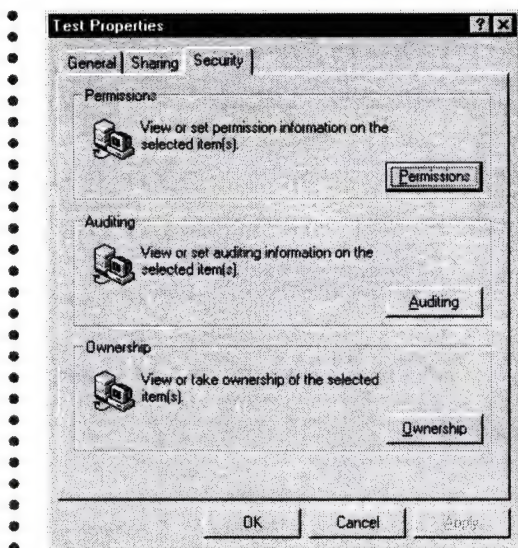
Права на доступ к файлам и каталогам определяют, может ли пользователь осуществлять к ним доступ и, если да, — как. Владение файлом или каталогом позволяет пользователю изменять права на доступ к нему. Владелец файла или каталога является его создатель. Администратор может вступить во владение файлом или каталогом без согласия владельца, но не может передать его обратно во владение прежнему владельцу. Чтобы передать владение файлом, администратор должен зарегистрироваться под именем другого пользователя и взять файл во владение.

Права на доступ к файлам и каталогам кумулятивны. Исключение составляет **No Access** (нет доступа), имеющее превосходство над остальными. Допустим, Саша имеет доступ к файлу FILE1 только на чтение. Одновременно он входит в группу Инженеры, обладающую правом изменения (**change**) файла FILE1. Значит, Саша может как читать, так и изменять файл FILE1. Если бы он был членом группы Бухгалтерия, не имеющей доступа к файлу, Саша тоже не имел бы доступа к этому файлу.

Предоставление прав на доступ к файлам и каталогам — основа защиты в Windows NT, управляемой пользователями. Права устанавливаются через меню **Security** в **File Manager**.

4.0

- В Windows NT 4.0 доступ ко всем диалоговым окнам, управляющим правами доступа, может осуществляться непосредственно из окон, соответствующих папкам, или из **Windows NT Explorer**. Для этого щелкните правой кнопкой мыши имя нужного файла или папки и в меню выберите пункт **Properties**. В появившемся диалоговом окне выберите вкладку **Security**.



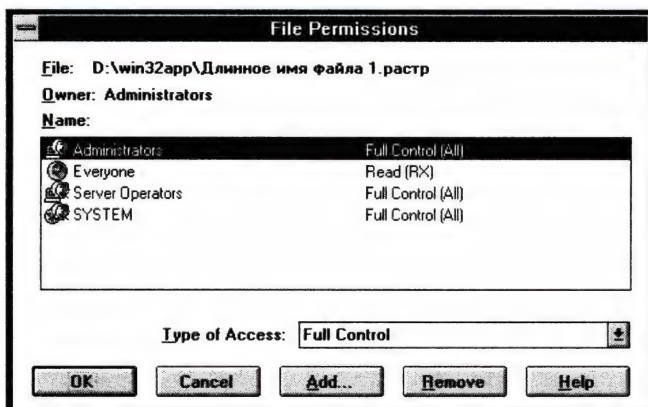
Диалоговое окно *File Properties*.

Предоставление прав на доступ к файлам

Чтобы ограничить доступ к файлу на разделе NTFS, его нужно выделить и в меню **Security** выбрать команду **Permissions** или щелкнуть кнопку на панели инструментов с изображением ключа. На экране появится диалоговое окно с элементами **File**, **Owner**, **Name** и **Type of Access**. Внизу также имеется ряд кнопок для добавления или исключения пользователей из списка доступа.



- В Windows NT 4.0 в диалоговом окне **File Properties** выберите вставку **Security** и "нажмите" кнопку **Permissions**. После этого появится описанное ниже диалоговое окно.



Диалоговое окно *File Permissions*.

File

Опция **File** отображает имя логического устройства, каталог NTFS и имя файла, к которому будут применены ограничения на доступ. Это именно тот файл, который был выделен в **File Manager**. Одновременно можно выделить несколько файлов.

Owner

Опция **Owner** (владелец) показывает текущего владельца файла. Данное диалоговое окно не позволяет изменить владельца. Для этого служит команда **Owner** из меню **Security** в **File Manager**. Чтобы изменить права на доступ к файлу, пользователь должен быть владельцем файла.

Name

В списке **Name** (имя) выводятся имена пользователей и групп, имеющих доступ к файлу, и тип доступа. Изначально права доступа наследуются от каталога, в котором расположен файл. Если одновременно выделено несколько файлов, отображаются права на доступ, общие для всех файлов. Права доступа делятся на две группы: права на каталог и права на файлы в каталоге. Например, установка **Add** и **Read** для каталога назначит права доступа к каталогу (RWX) — чтение, запись и исполнение; файл в этом каталоге получит права доступа (RX), т.е. только чтение и исполнение. В таблице перечислены сокращения для разных типов доступа.

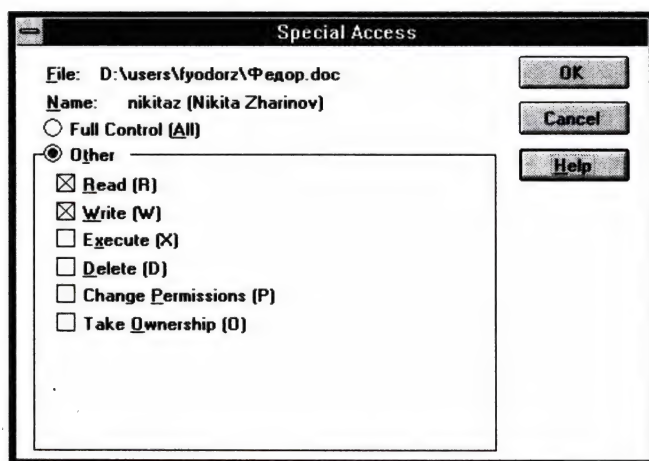
Право доступа	Сокращение
Read (чтение)	R
Delete (удаление)	D
Write (запись)	W
Change Permission (изменение прав)	P
Execute (исполнение)	X
Take Ownership (вступление во владение)	O

Type of Access

В этом списке можно выбрать основные типы доступа к файлам и связанные с ними действия над файлами. В таблице показаны типы доступа и операции над файлами.

● — <i>разрешено</i>	<i>No Access</i>	<i>Read</i>	<i>Change</i>	<i>Full Control</i>
Показывать данные файла		●	●	●
Показывать атрибуты файла		●	●	●
Исполнять файл, если это программа		●	●	●
Показывать владельца файла и типы доступа		●	●	●
Изменять атрибуты файла			●	●
Изменять и добавлять данные в файл			●	●
Удалить файл			●	●
Изменять владельца файла и права доступа				●

В списке доступа имеется элемент **Special Access** (Специальный доступ). Выбрав его, Вы выведете на экран диалоговое окно **Special Access** с флажками, позволяющими установить специальный вид доступа.



Диалоговое окно *Special Access*.

Специальный вид доступа можно установить для любого файла или группы файлов. В приведенной ниже таблице перечислены специальные виды доступа и связанные с ними действия.

	READ	WRITE	EXECUTE	DELETE	Change Permissions Take Ownership
Показывать владельца файла и права доступа	✓	✓	✓		
Показывать данные в файле	✓				
Показывать атрибуты файла	✓		✓		
Изменять атрибуты файла		✓			
Изменять и добавлять данные к файлу	✓	✓			
Выполнять файл, если это программа			✓		
Удалять файл				✓	
Изменять права доступа к файлу					✓
Вступать во владение файлом					✓

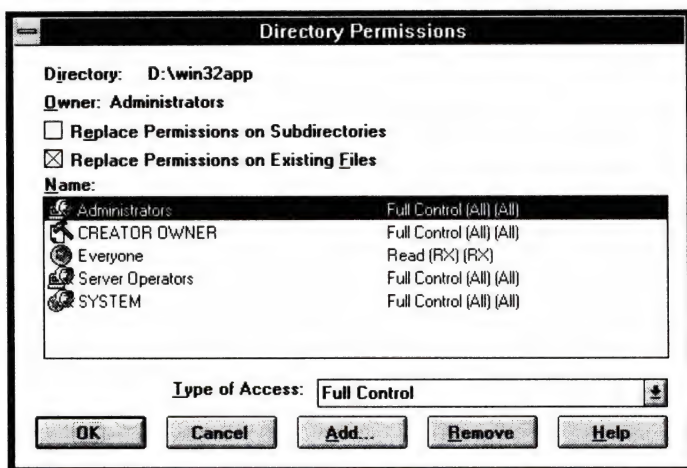
Кстати: Опишем ситуацию, таящую в себе большую опасность. Существует вероятность того, что администратор системы в порыве рвения “за полную защищенность” захочет запретить всем (**Everyone**) доступ к системным файлам. (Напомню: запрещение доступа группе Everyone означает запрещение доступа учетной записи **SYSTEM**, под которой действует операционная система.) Система сообщит о тяжелых последствиях такой операции, однако администратор все-таки может установить запрет доступа. И тогда в следующий раз операционная система не загрузится. Чтобы восстановить работоспособность, выполните процедуру **Repair** и воспользуйтесь **Emergency Repair Disk** (см. раздел **Emergency Repair Disk**).

Предоставление прав на доступ к каталогам

Для ограничения доступа к каталогу на разделе NTFS выделите его и выберите команду **Permissions** в меню **Security** или щелкните на панели инструментов кнопку с изображением ключа.

В Windows NT 4.0 в диалоговом окне **File Properties** выберите вкладку **Security** и “нажмите” кнопку **Permissions**.

На экране появится диалоговое окно **Directory Permissions** с элементами **Directory**, **Owner**, **Replace Permissions on Subdirectories**, **Replace Permissions on Existing Files**, **Name** и **Type of Access**. Кнопки внизу позволяют добавлять или исключать пользователей из списка доступа.



Диалоговое окно *Directory Permissions*.

Directory

Опция **Directory** отображает имя логического устройства и каталог NTFS, к которому будут применены ограничения на доступ. Это именно тот каталог, который был выделен в **File Manager**. Одновременно можно выделить несколько каталогов.

Owner

Опция **Owner** (владелец) показывает текущего владельца каталога. Это диалоговое окно не позволяет изменить владельца. Для этого выберите команду **Owner** в меню **Security** в **File Manager**. Чтобы изменять права на доступ к каталогу, пользователь должен быть владельцем каталога.

Replace Permissions on Subdirectories

Если пользователь хочет изменить права только на выбранный каталог и файлы в нем, то этот флажок помечать не надо. А если те же права доступа надо применить ко всем вложенным каталогам, пометьте его. По умолчанию он не помечен.

Replace Permissions on Existing Files

Эта опция позволяет изменять права на доступ одновременно к каталогу и файлам, находящимся в нем. По умолчанию флажок помечен.

Name

В списке **Name** (имя) отображаются имена пользователей и групп, имеющих доступ к каталогу, и тип доступа. Администратор может добавлять

новых пользователей или группы в список, используя кнопки **Add** (Добавить) или **Remove** (Убрать).

Type of Access

В этом списке приведены все возможные права на доступ. В следующих таблицах перечислены права на доступ к каталогам и связанные с ними действия, применимые к каталогам и файлам.

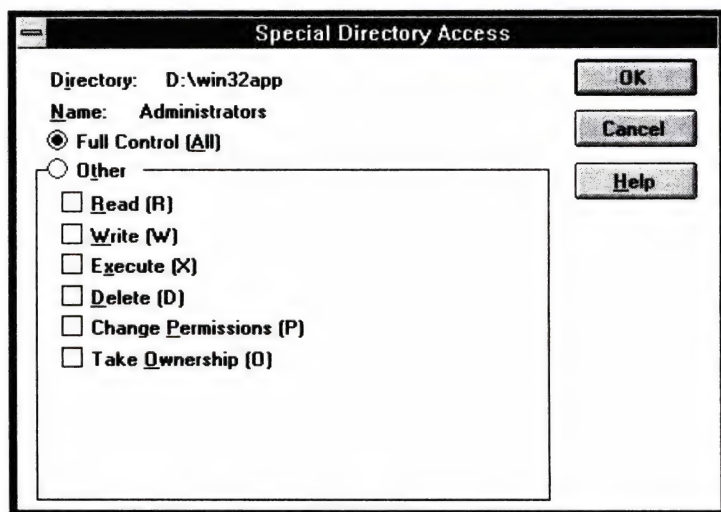
Права доступа к каталогам и действия над каталогами

	No Access	List	Read	Add	Add&Read	Change	Full Control
Показывать имена каталогов		✓	✓		✓	✓	✓
Показывать атрибуты каталогов		✓	✓	✓	✓	✓	✓
Переходить в подкаталоги		✓	✓	✓	✓	✓	✓
Изменять атрибуты каталога				✓	✓	✓	✓
Создавать подкаталоги и добавлять файлы				✓	✓	✓	✓
Показывать владельца каталога и права доступа		✓	✓	✓	✓	✓	✓
Удалять каталог						✓	✓
Удалять любой файл или пустой подкаталог в каталоге							✓
Вступать во владение каталогом							✓
Изменить права доступа к каталогу							✓

Права доступа к каталогам и действия над файлами

	No Access	List	Read	Add	Add&Read	Change	Full Control
Показывать владельца файла и права доступа			✓		✓	✓	✓
Показывать данные в файле			✓		✓	✓	✓
Показывать атрибуты файла			✓		✓	✓	✓
Изменять атрибуты файла			✓		✓	✓	✓
Изменять и добавлять данные к файлу						✓	✓
Выполнять файл, если это программа						✓	✓
Удалять файл						✓	✓
Изменять права доступа к файлу							✓
Вступать во владение файлом							✓

В дополнение к этим стандартным типам доступа можно выбрать в списке пункты **Special Directory Access** (Особый доступ к каталогу) и **Special File Access** (Особый доступ к файлу). Выбор последнего выводит диалоговое окно **Special Directory Access**.



Диалоговое окно *Special Directory Access*.

Особые права доступа можно установить как на целый каталог, так и на отдельные файлы в нем. В таблице перечислены особые права доступа к каталогам и связанные с ними действия над каталогами.

	READ	WRITE	EXECUTE	DELETE	Change Permissions	Take Ownership	Full Control
Показывать имена файлов в каталоге	✓						✓
Показывать атрибуты каталогов	✓		✓				✓
Добавлять файлы и подкаталоги		✓					✓
Изменять атрибуты каталога		✓					✓
Переходить в подкаталоги			✓				✓
Показывать владельца каталога и права доступ	✓	✓	✓				✓
Удалять каталог				✓			✓
Изменять права на доступ к каталогом					✓		✓
Вступать во владение каталогомъ						✓	✓

Отмечу некоторые уникальные ситуации:

- Существуют случаи, когда права на доступ к каталогу для пользователя или группы не передаются в подкаталоги. Это происходит, когда права предоставлены через группу **Creator Owner**. Права доступа, которые не будут унаследованы подкаталогами, отмечаются звездочкой.
- Для некоторых прав доступа к каталогу устанавливается право доступа к файлам **Not Specified** (не указаны). Когда доступ к файлам, предоставленный пользователю или группе, не указан, группа или пользователь не могут использовать файлы в каталоге, пока им не будут предоставлены права другими средствами, например, путем назначения прав доступа к отдельным файлам.
- Устанавливая права на доступ к каталогу, через специальную группу **Creator Owner** можно предоставить доступ только к тем файлам и подкаталогам, что были созданы пользователями внутри этого каталога. Права, установленные для **Creator Owner**, передаются пользователю, создающему файлы и подкаталоги внутри каталога. Например, для каталога назначен доступ **Add&Read** для группы **Everyone** и **Change** — для группы **Creator Owner**. Если Дима добавит файлы в каталог, он сможет изменять и удалять их, в то время как остальные смогут их только просматривать.

Владение каталогами и файлами

По умолчанию создатель каталога или файла является его владельцем. Нельзя передать файл или каталог кому-либо во владение, однако владелец файла может предоставить кому-либо право вступить во владение. У администраторов всегда есть возможность вступить во владение файлом или каталогом. Файл или каталог всегда находятся под контролем его владельца, который может менять права на доступ. Чтобы узнать владельца файла или каталога, применяется команда **Owner** в **File Manager**.

4.0

В Windows NT 4.0 в диалоговом окне **File Properties** выберите вкладку **Security** и "нажмите" кнопку **Owner**.

В появляющемся диалоговом окне отображаются имя выбранного файла или каталога, текущий владелец и кнопка **Take Ownership**, позволяющая вступить во владение при наличии соответствующих прав.



Диалоговое окно *Owner*.

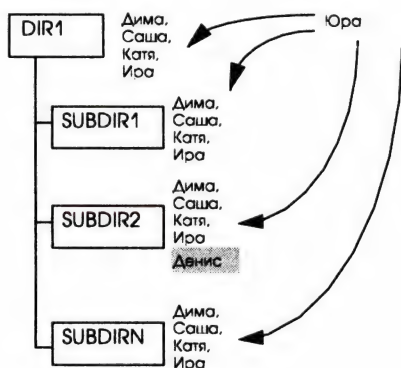
Правами, предоставляющими возможность вступать во владение, являются:

- Full Access;
- Special Access, включающий Take Ownership;
- Административные права.

Стратегия предоставления прав на доступ

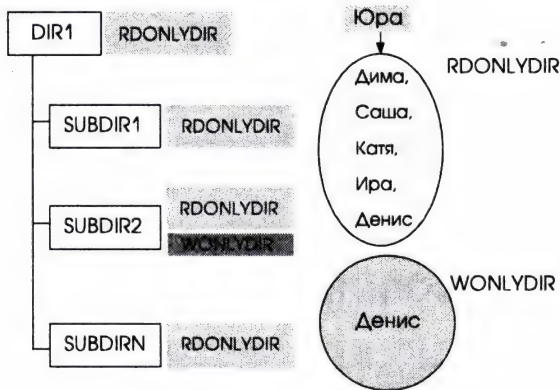
Права на доступ следует предоставлять только группам, а не отдельным пользователям. Предоставление прав группам упрощает управление сервером. Если нескольким пользователям нужен определенный тип доступа, их объединяют в группу и предоставляют права этой группе.

Рассмотрим пример. Допустим, имеется каталог DIR1, а в нем несколько подкаталогов SUBDIR1...SUBDIRN. Дима, Саша, Катя и Ира должны иметь доступ только на чтение к каталогу DIR1 и всем его подкаталогам, а Денис — еще и на запись к подкаталогу SUBDIR2. Можно, конечно, каждому из перечисленных пользователей предоставить необходимые права доступа. Но тогда дальнейшее администрирование будет затруднено. Чтобы, скажем, предоставить доступ ко всем каталогам только на чтение еще и Юре, придется выполнять эту операцию для каждого из подкаталогов в отдельности: ведь, отметив флажок **Replace Permissions on Subdirectories** при назначении прав доступа к каталогу DIR1, мы лишим Дениса возможности записи в каталог SUBDIR2.



Кроме того, если даже ко всем вложенным подкаталогам применимы одни и те же права доступа, предоставление прав новому пользователю может стать весьма длительной операцией при большом количестве файлов в подкаталогах. Группы значительно облегчают эту задачу. Создавая структуру каталогов, стоит заранее подумать о правах доступа к ней и сформировать группы пользователей. Применительно к рассмотренному выше примеру

достаточно иметь всего 2 группы, например RDONLYDIR — для пользователей с правом доступа только на чтение и WONLYDIR — для имеющих право записи. И тогда предоставление Юре доступа на чтение всех подкаталогов сведется к его включению в группу RDONLYDIR.



Использование прав на доступ на разделах FAT и HPFS

На томах с FAT или HPFS нет возможности назначить права доступа к отдельным файлам или каталогам. Единственная возможность ограничить доступ — ограничение доступа к каталогам, предоставляемым в совместное использование в сети. В этом случае ограничения распространяются только на пользователей, осуществляющих доступ к предоставляемому ресурсу по сети. При этом существует четыре вида доступа: **Full Control of Files/Directories** (полный контроль над файлами или каталогами), **Change Files/Directories** (изменение файлов или каталогов), **Read Files/Directories** (чтение файлов или каталогов) и **No Access to Files/Directories** (отсутствие доступа к файлам или каталогам).

Нет необходимости указывать **No Access** для всех пользователей, которым запрещен доступ к каталогу. Непредоставление пользователю или группе, к которой он принадлежит, прав доступа эквивалентно запрету на доступ. **No Access** применяется, когда пользователи или группы могут получить доступ к каталогу другими средствами. Например, можно разрешить доступ к совместно используемому каталогу всем, кроме группы Бухгалтерия, предоставив группе **Everyone** полный доступ (**Full Control**), а группе Бухгалтерия — **No Access**.

File Delete child

Право доступа **Full Control** включает в себя “скрытое” право — **FDC (File Delete child)**. Все пользователи, обладающие правом доступа к каталогу **Full Control**, могут удалять файлы в корне каталога. Единственный способ запре-

тить данную возможность — предоставить особый доступ (*Special Access*) вместо полного доступа к каталогам.

FDC можно рассматривать как выделенный, но скрытый дополнительный флажок в диалоговом окне *Special Directory Access*, который отмечается при выборе *Full Control*.

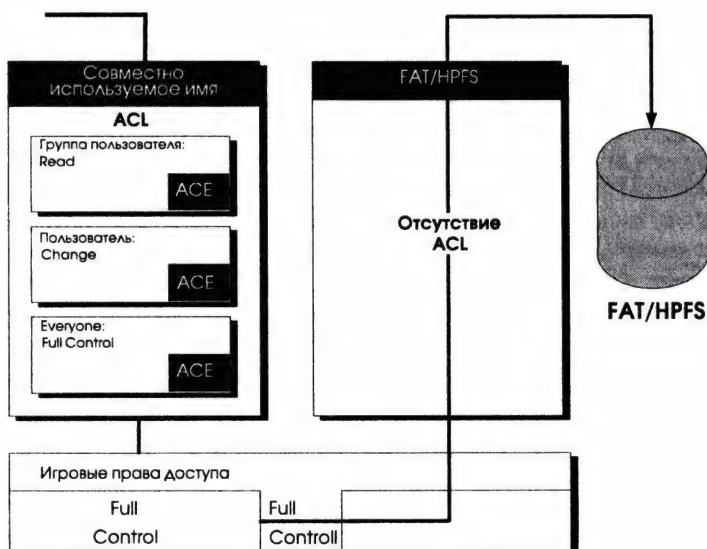
Право **FDC** включено для совместимости с POSIX. Согласно спецификациям POSIX, пользователь, имеющий право записи в каталог должен обладать возможностью удаления файлов в каталоге независимо от прав, назначенных для этих файлов. Это применимо только к файлам, находящимся в каталоге, но не в подкаталогах.

Совместное использование в сети

Защита каталогов, предоставляемых в совместное использование, состоит из двух уровней: сетевого (доступ к совместно используемым каталогам) и локального (доступ к файлам и каталогам, расположенным на томе NTFS).

Защита предоставляемых для совместного использования каталогов на томах FAT или HPFS

Файловые системы FAT и HPFS не предоставляют возможностей локальной защиты, и поэтому защита каталогов на них доступна только на сетевом уровне.



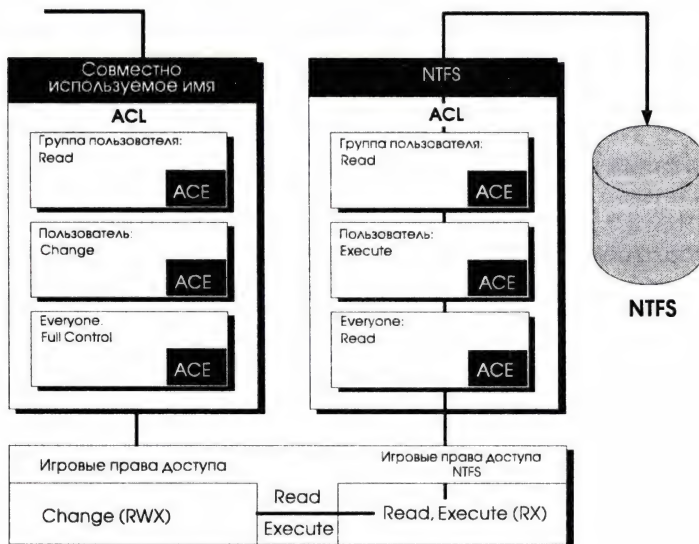
Ограничение доступа — FAT/HPFS.

Защита предоставляемых для совместного использования каталогов на томах NTFS

На томах NTFS локальная защита возможна. Поэтому удаленный пользователь получает права доступа, являющиеся комбинацией прав на доступ к совместно используемым ресурсам и локальных ограничений NTFS.

Если удаленному пользователю необходимо записывать в файлы или удалять файлы, расположенные на разделе NTFS, то и локальные ограничения, и ограничения на совместное использование должны позволять это. Например, Оля имеет права доступа к совместно используемому каталогу типа **Change**. Однако локально для нее назначены права **Read** и **Execute**. Значит, Оля может только читать и исполнять файлы, но не писать в них или удалять.

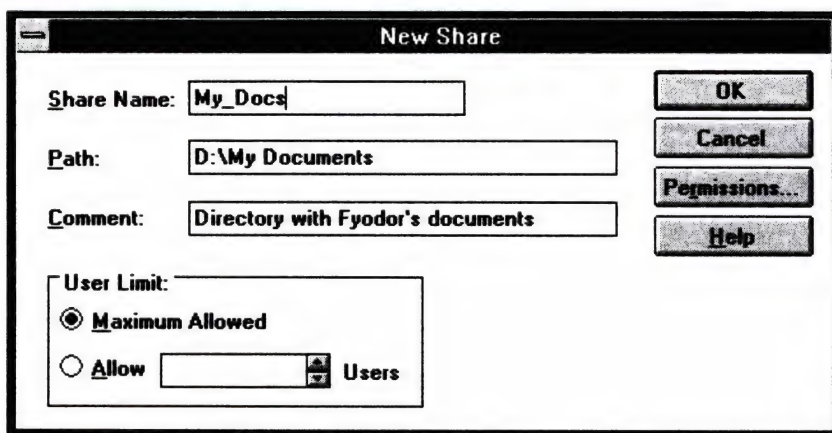
Когда сетевой администратор создает новый подкаталог на NTFS, группа **Everyone** автоматически получает на него право **Full Control**. Это делает новый ресурс равным по доступу ресурсу, расположенному на разделе FAT или HPFS. Поэтому администратору лучше, исключив группу **Everyone** из списка доступа к ресурсу, создать вместо нее конкретные группы с определенными правами.



Ограничение доступа — NTFS.

Предоставление файлов и каталогов в совместное использование

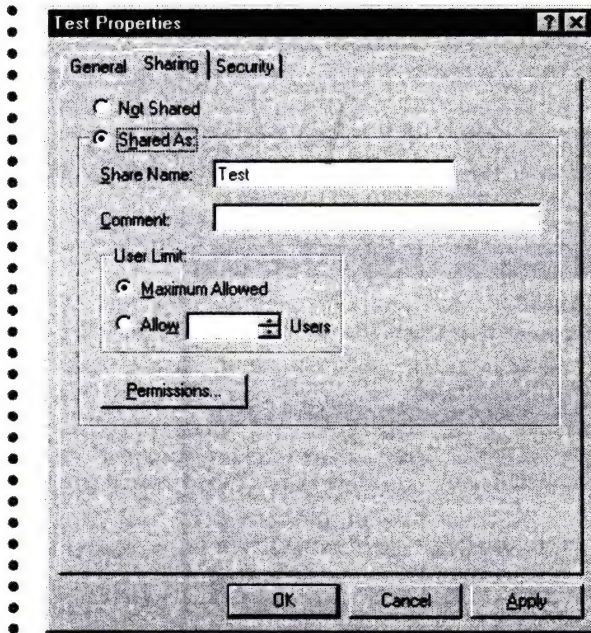
Предоставление файлов и каталогов в совместное использование в сети выполняется в File Manager командами меню **Disk**. Каталог можно предоставить в совместное использование независимо от того, на каком разделе диска он расположен — FAT, HPFS или NTFS. Чтобы предоставлять каталоги в совместное использование, пользователь должен быть зарегистрирован как член группы **Administrators** или **Server Operators**. Команда **Share As** в меню **Disk** выводит диалоговое окно **New Share**, описание элементов которого приведено ниже.



Диалоговое окно *New Share*.



- В Windows NT 4.0 для предоставления каталога в совместное использование необходимо, щелкнув его имя правой кнопкой мыши, выбрать в меню команду **Sharing**. Вслед за этим сразу появится диалоговое окно **File Properties** с активной вкладкой **Sharing**.



Диалоговое окно *Directory Properties* с активной вкладкой *Sharing*.

Share Name

Показывает имя, которое должны указывать пользователи для подключения к совместно используемому ресурсу. По умолчанию **File Manager** использует имя каталога, однако не стоит забывать, что не все имена доступны для пользователей, подключенных по сети и работающих под MS-DOS. Если введенное Вами имя не соответствует этим требованиям, появится соответствующее предупреждение.

Path

Показывает путь к каталогу, предоставляемому в совместное использование.

Comments

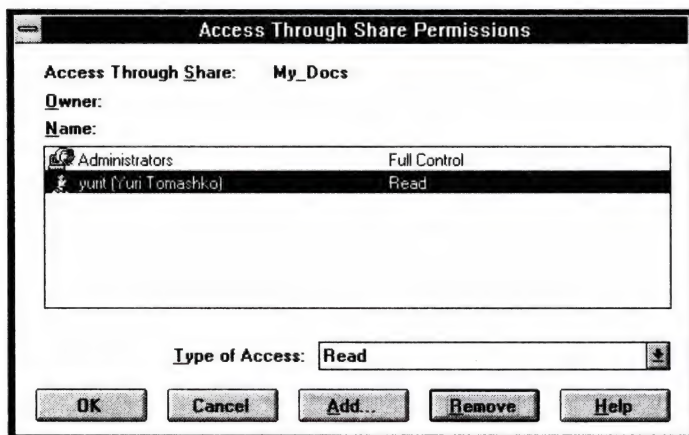
В это поле можно ввести комментарий. Основное назначение — информационное. Комментарии помогут удаленным клиентам легче ориентироваться при просмотре доступных ресурсов.

User Limit

Позволяет установить ограничение на максимальное число пользователей, осуществляющих одновременный доступ к ресурсу. По умолчанию ограничения не накладываются.

Permissions

Кнопка **Permissions** выводит диалоговое окно **Access Through Share Permissions**. В нем показаны имя предоставляемого ресурса, его владелец и список пользователей и групп с указанием прав доступа к ресурсу. Кнопками **Add** и **Remove** можно добавлять новых пользователей или исключать имеющихся. Тип доступа выбирается из списка **Type of Access**.



Диалоговое окно *Access Through Share Permissions*.

В таблице показаны основные права доступа, предоставляемые в диалоговом окне **Access Through Share Permissions**, и соответствующие им действия над файлами и каталогами.

	No Access	Read	Change	Full Control
Показ имен файлов и подкаталогов		•	•	•
Показ данных в файлах и их атрибутов	•	•	•	
Выполнение программ		•	•	•
Переход в подкаталоги		•	•	•
Создание подкаталогов и файлов			•	•
Изменять и добавлять данные в файлы		•	•	
Изменять атрибуты файла			•	•
Удалять файл и подкаталоги			•	•
Изменять права доступа (только на NTFS)			•	
Вступать во владение (только на NTFS)			•	

При этом помните, что, кроме прав, предоставленных для совместно используемого каталога, активными остаются права на доступ к файлам и каталогам на томе NTFS.

Для эффективного администрирования ресурсов, предоставляемых для совместного использования, надо помнить о некоторых особенностях:

- Права доступа, установленные для совместно используемого ресурса, применимы к каталогу, подкаталогам и всем файлам в каталоге.
- Windows NT автоматически создает совместно используемые ресурсы для административного и системного использования. Сразу после старта Windows NT в совместное использование администраторами предоставляются корневые каталоги всех дисков и системный каталог, например C:\WINNT35. Имя ресурса для диска состоит из буквы, присвоенной диску, и знака доллара (например, C\$). Для системного каталога имя ресурса ADMIN\$. Кроме того, создается совместно используемый ресурс NETLOGON, указывающий на тот каталог, где находятся файлы сценариев регистрации. По умолчанию это каталог:

```
<системный каталог>\SYSTEM32\REPL\IMPORT\SCRIPTS
```

Еще одним совместно используемым административным ресурсом является REPL\$, используемый службой тиражирования. Он указывает на каталог:

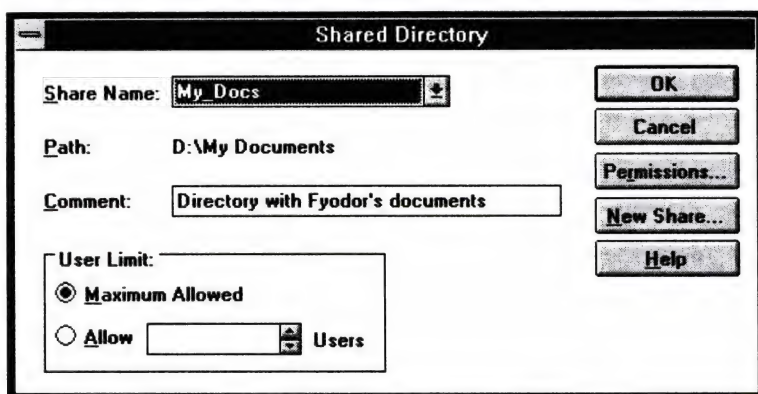
```
<системный каталог>\SYSTEM32\REPL\EXPORT
```

К административным ресурсам могут подключаться только члены групп **Administrators**, **Server Operators** или **Backup Operators**. Только члены группы **Administrators** могут изменять свойства этих ресурсов.

Повторное предоставление ресурсов в совместное использование

Один и тот же каталог может быть предоставлен в совместное использование несколько раз. При этом каждый раз применяется новое имя ресурса и можно указать другие права доступа для других групп пользователей.

Для повторного предоставления каталога выделите его в **File Manager** и выберите команду **Share As** в меню **Disk**. В появившемся диалоговом окне **Shared Directory** можно изменить права доступа к существующему ресурсу или создать новый.



Диалоговое окно *Shared Directory*.

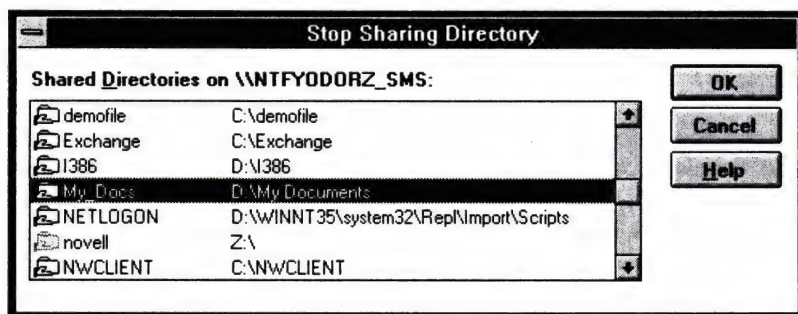
Новый совместно используемый ресурс создается щелчком кнопки **New Share**.



- В Windows NT 4.0 для повторного предоставления каталога в совместное использование, щелкнув его имя правой кнопкой мыши, выберите в меню команду **Sharing**. В появившемся диалоговом окне **File Properties** с активной вкладкой **Sharing** будет указано имя, под которым данный каталог уже предоставлен в совместное использование.

Просмотр предоставленных ресурсов и отмена совместного использования

Любой член группы **Administrators** или **Server Operators** имеет возможность просмотра ресурсов и отмены их совместного использования. Эта функция возможна при выборе команды **Stop Sharing Directory** в меню **Disk** в **File Manager**.



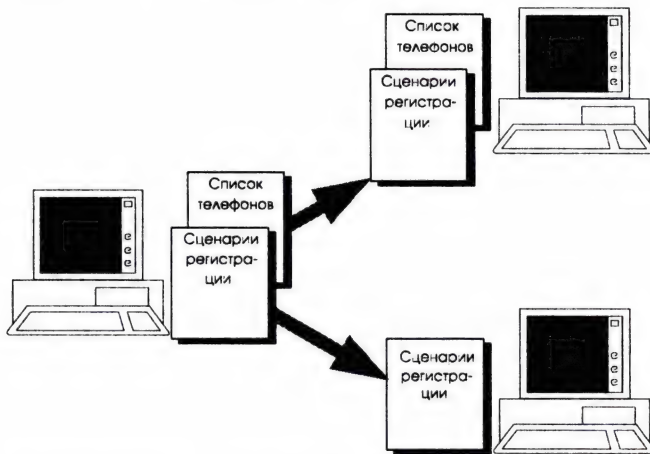
Диалоговое окно *Stop Sharing Directory*.

В этом диалоговом окне показано имя компьютера, перечислены имена ресурсов и полные пути к ним. Для прекращения совместного использования ресурсов выделите их в списке и нажмите кнопку **OK**. Если в этот момент ресурс используется сетевым клиентом, **File Manager** выведет соответствующее предупреждение.

Некоторые ресурсы в этом списке могут быть показаны блеклыми. Это связано с тем, что фактически данный ресурс уже не существует, хотя его имя по-прежнему появляется в списке совместно используемых ресурсов для сетевых клиентов. Обычно это происходит при удалении каталога, предоставленного в совместное использование.

Тиражирование каталогов

Средства тиражирования позволяют поддерживать идентичность файлов и каталогов на нескольких серверах или рабочих станциях.



Тиражирование сценариев регистрации.

Данная функция позволяет упростить работу с файлами, а также балансировать загрузку между серверами. Разгрузка сервера достигается за счет того, что необходимые файлы находятся не на одном сервере. Упрощение работы с файлами заключается в автоматическом обновлении файлов на разных компьютерах.

Windows NT Workstation может только импортировать данные, а Windows NT Server — и импортировать, и экспортировать в процессе тиражирования.

Процесс тиражирования состоит по крайней мере из двух компонентов: сервера экспорта и компьютера(ов) импорта. Сервером экспорта может быть Windows NT Server. На этой системе должны содержаться файлы, тиражируе-

мые на компьютер импорта. В качестве компьютера импорта могут выступать Windows NT Server, Windows NT Workstation или LAN Manager Server.

Чтобы тиражирование стало возможным, экспортируемые файлы должны храниться в каталоге экспорта, . приниматься компьютерами в каталоги импорта. По умолчанию каталогом экспорта является:

```
<системный каталог>\SYSTEM32\REPL\EXPORT
```

Каталогом импорта по умолчанию является:

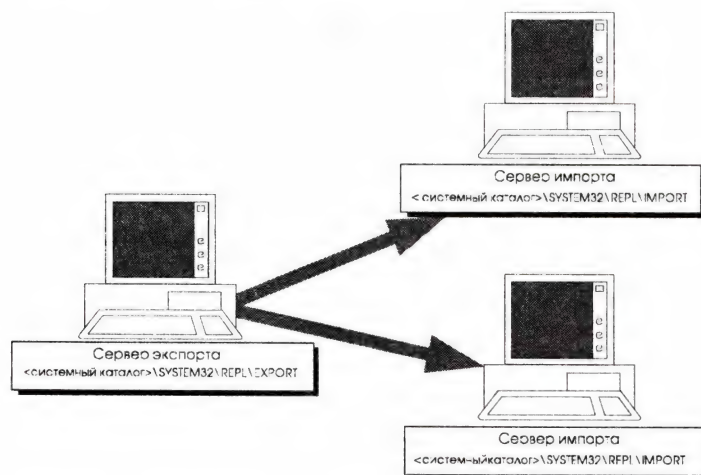
```
<системный каталог>\SYSTEM32\REPL\IMPORT
```

Для тиражирования сценариев регистрации, однако, используются специальные каталоги. Для экспорта это:

```
<системный каталог>\SYSTEM32\REPL\EXPORT\SCRIPTS
```

а для импорта:

```
<системный каталог>\SYSTEM32\REPL\IMPORT\SCRIPTS
```



Каталоги экспорта и импорта.

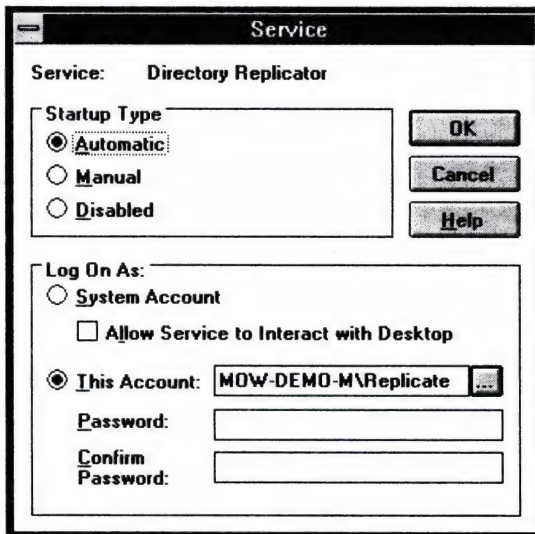
Конфигурирование компьютеров экспорта и импорта

Прежде чем запустить сервис тиражирования каталогов, необходимо:

- > создать учетную запись для тиражирования;
- > активизировать сервис **Directory Replicator**.

Учетной записи, обслуживающей услугу тиражирования, должна быть обеспечена возможность работы в любое время. Отметьте флажок **Password Never Expires** и сбросьте флажок **User Must Change Password At Next Logon**. Дополнительно к этому необходимо группе **Replicator** домена предоставить право **Log On As a Service**. Учетная запись должна входить в группы **Backup Operators**, **Domain Users** и **Replicator**.

Необходимо сконфигурировать автоматический запуск сервиса **Directory Replicator**, а также его регистрацию на серверах экспорта через созданную учетную запись. Это выполняется, например, в программе **Server Manager**.



Диалоговое окно *Directory Replicator Service*.

Компьютер импорта также необходимо сконфигурировать для приема тиражируемых файлов и каталогов. Для рабочих станций Windows NT Workstation, входящих в доверяющий домен, включите в локальную группу **Replicator** глобальную группу **Replicator** сервера экспорта, а также предоставьте локальной группе **Replicator** привилегии **Log On As A Service**. Для всех систем импорта служба тиражирования должна быть сконфигурирована на автоматический запуск и регистрацию через учетную запись, созданную на сервере экспорта. Дополнительно сервер импорта должен быть сконфигурирован на прием файлов с других серверов домена. Это выполняется в программе **Server Manager**.

Тиражирование лучше всего выполнять для файлов, используемых только для чтения. Любой файл или каталог, расположенный в каталоге импорта и модифицированный пользователем, будут переписаны службой тиражирования. Примерами файлов, подлежащих тиражированию, являются сценарии регистрации, профили пользователей, загрузочные файлы клиента Systems Management Server.

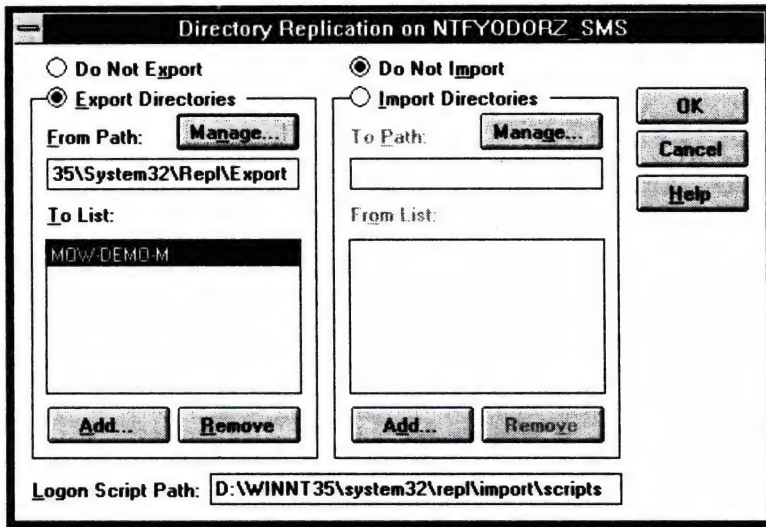
Защита тиражирования

Защита тиражирования устанавливается в **Server Manager**. В диалоговом окне **Directory Replication** на сервере экспорта пользователь может:

- определить каталог экспорта;
- запретить экспорт из каталога;
- запретить экспорт подкаталога в каталоге;
- отслеживать дату и время запрета экспорта каталога,

а в диалоговом окне **Directory Replication** на сервере импорта:

- указать путь к каталогу, где будут храниться тиражированные файлы;
- определить путь;
- запретить импорт в каталог;
- отслеживать состояние и эффект от обновлений;
- отслеживать дату и время обновления файлов в каталоге импорта.

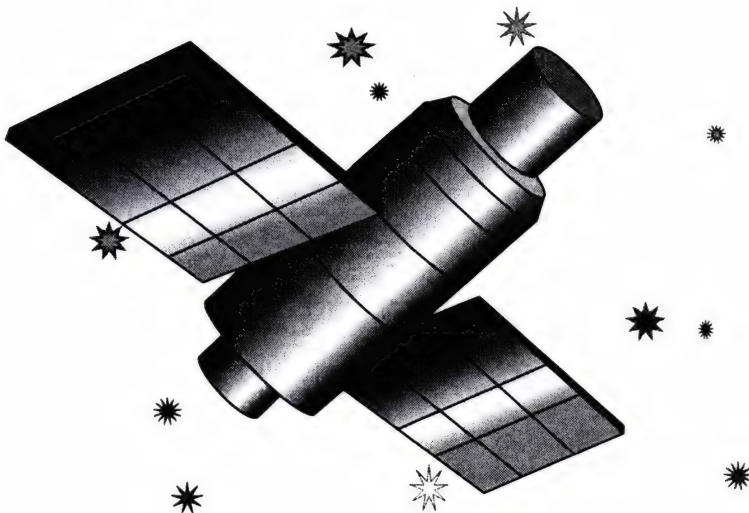


Диалоговое окно Directory Replication.

Служба тиражирования может вызвать серьезные нарушения защиты при неправильном администрировании. Если тиражирование выполняется на компьютер, находящийся в сети, администратор должен быть точно уверен, какие группы пользователей имеют доступ к каталогу импорта. Дополнительно очень важно назначить пароль для учетной записи, используемой службой тиражирования. Если пароль не назначить, это может стать путем для неавторизованного входа в систему.

Обеспечение отказоустойчивости

Если Вы слепо доверяете надежности “винчестера”, то можете не сомневаться: наступит день, когда Вы об этом пожалеете. У любой механической системы (а жесткий диск таковой и является) есть свой запас прочности. Что произойдет после выработки ресурса, точно никто не скажет, но я ставлю свой “ноутбук” против счетных палочек: самая важная для Вас информация пропадет безвозвратно. В Windows NT Server встроены механизмы, обеспечивающие отказоустойчивость системы: средства особо надежной работы с диском, резервного копирования на магнитную ленту, поддержки работы с источниками бесперебойного питания, выбор работоспособной конфигурации и восстановление системы со специального диска. Однако компьютер сам по себе тоже может выйти из строя. Чтобы этот факт не отразился на Вашей работе, необходимо использовать кластерные решения.



Средства повышения надежности работы с диском

Если Вы регулярно пользовались программами вроде CHKDSK или Norton disk Doctor, то наверняка знаете, что иногда они обнаруживают на жестких дисках "плохие области" (bad blocks), которые помечают как недоступные. Причин появления таких областей хватает: от некачественного диска до вирусов. Но что бы там ни было, результат всегда один — сокращение доступного рабочего пространства на диске. Если своевременно не протестируйте диск, последствия могут быть более печальными: Вы потеряете данные, записанные в поврежденный участок, или еще хуже: операционная система станет неработоспособной. Поэтому если в Вашем компьютере только один жесткий диск или Вы не используете технологии, описанные далее в этой главе, Ваша первейшая обязанность — регулярная проверка состояния диска.



- **Замечание:** Современные компьютерные системы, выпускаемые известными производителями техники, зачастую обладают встроенными средствами контроля за состоянием дисков и оповещения операционной системы и администратора о надвигающейся угрозе. Примером могут служить компьютеры Compaq Proliant, в которых о предстоящем крахе диска извещается как операционная система, так и оператор — предупреждающим сигналом, посылаемым на пейджер.

Проверка состояния жесткого диска

Для проверки состояния жесткого диска используется встроенная утилита CHKDSK, запускаемая из командной строки. Для поиска плохих секторов она запускается с ключом /R. Эта операция может продолжаться несколько часов. Если Вы выполняете эту операцию регулярно, то о наличии сбойных секторов можно косвенно судить по резко возросшему времени выполнения проверки.

```
CHKDSK [drive:][[path]filename] [/F] [/V] [/R] [/L[:size]]
```

[drive:] Specifies the drive to check.

filename Specifies the file(s) to check for fragmentation (FAT only).

/F Fixes errors on the disk.

/V Displays the full path and name of every file on the disk.

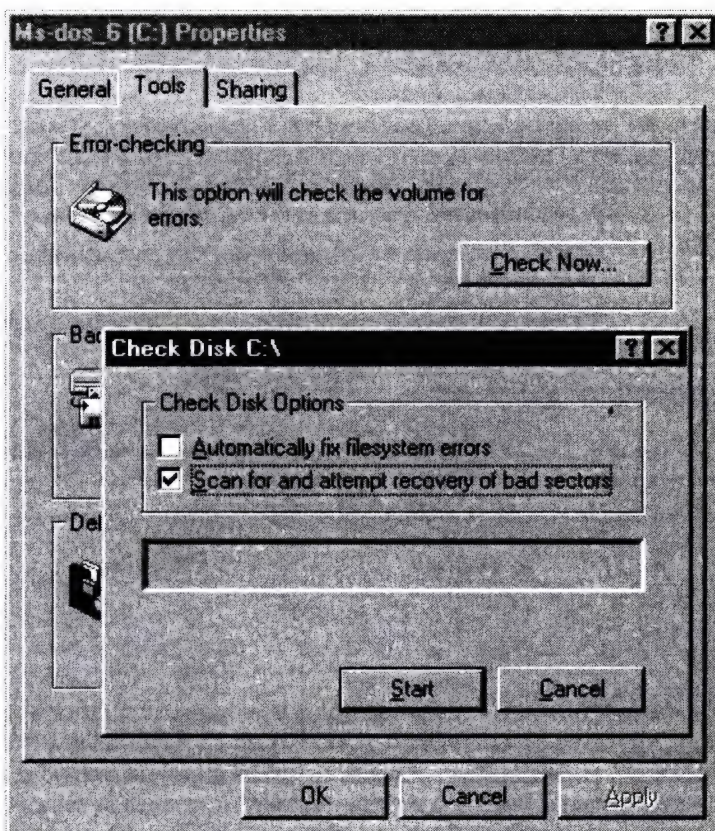
/R Locates bad sectors and recovers readable information.

/L:size NTFS only: changes the log file size to the specified number of kilobytes. If size is not specified, displays current size

4.0

Замечание: Если во время работы системы выполнение программы **CHKDSK** невозможно (например, на выбранном диске находится файл своппинга), Вам будет предложено перенести ее исполнение на момент загрузки системы. В случае Вашего согласия при следующей перезагрузке будет выполнена полная проверка диска.

В Windows NT 4.0 встроена графическая утилита проверки диска. Для ее вызова щелкните правой кнопкой мыши имя диска в папке **Мой компьютер** и в появившемся меню выберите команду **Properties**. В диалоговом окне щелкните вкладку **Tools** и "нажмите" кнопку **Check Now**. Для полной проверки диска в диалоговом окне **Check Disk** отметьте оба флажка: **Automatically fix filesystem errors** и **Scan for and attempt recovery of bad sectors**.



Диалоговое окно проверки состояния жестких дисков.

Чтобы обезопасить себя от неприятностей, связанных с ненадежной работой дисковой системы, на сервере необходимо использовать средства, повышающие ее надежность. К таким средствам Windows NT относятся зеркализация дисков, дублирование дисков, чередование дисков с контролем четности и замена секторов (в "горячем" режиме).

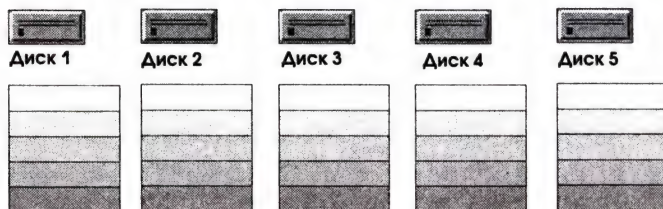
Технология RAID (Избыточный массив недорогих дисков)

Средства повышения надежности работы с дисками стандартизованы в промышленности и подразделяются на 7 уровней использования избыточных массивов недорогих дисков (RAID). У каждого из уровней свой набор значений производительности, надежности и стоимости. В Windows NT Server обеспечивается поддержка RAID уровней 0 — 5.

Уровни	RAID
Уровень 0	Чередование дисков
Уровень 1	Зеркализация дисков
Уровень 2	Чередование дисков с записью кода коррекции
Уровень 3	Чередование дисков с записью кода коррекции в виде четности
Уровень 4	Чередование дисков большими блоками с записью четности на одном диске
Уровень 5	Чередование дисков с записью четности на нескольких дисках

Чередование дисков

Чередование дисков (RAID 0) обеспечивает чередование между различными разделами диска. При этом файл как бы "размазывается" по нескольким физическим дискам. Этот метод может увеличить производительность работы с диском, особенно когда диски подключены к разным контроллерам дисков. Так как этот метод не обеспечивает избыточности, его нельзя назвать в полной мере RAID. При выходе из строя любого раздела в таком массиве все данные будут потеряны. Для реализации метода требуется от 2 до 32 дисков. Увеличение производительности достигается только при использовании разных контроллеров диска.



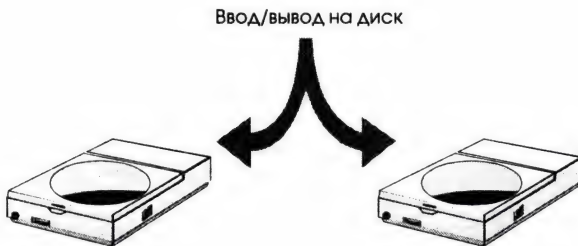
Уровень 0 — Чередование дисков.

Зеркализация и дублирование дисков

Создание зеркальной копии диска или раздела осуществляется средствами RAID 1: зеркализацией или дублированием. Зеркальное отражение дисков действует на уровне разделов. Любой раздел, включая загрузочный или системный, может быть зеркально отражен. Это простейший метод повышения надежности работы с диском. Зеркализация — самый дорогой способ обеспечения надежной работы с дисками, так как при этом задействовано лишь 50% объема жесткого диска. Однако в большинстве одноранговых или небольших серверных сетях такой способ является самым дешевым за счет использования всего двух дисков. Для обеспечения уровней RAID 3 и выше требуется не менее 3 жестких дисков.

Дублирование дисков — зеркализация с применением дополнительного адаптера на вторичном дисковом — обеспечивает отказоустойчивость и при сбое контроллера, и при сбое диска. Кроме того, дублирование может повысить и производительность.

Подобно зеркализации, дублирование выполняется на уровне раздела. Для Windows NT нет разницы между зеркализацией и дублированием. Это просто вопрос местонахождения другого раздела.



Зеркализация дисков.

При зеркализации системного загрузочного диска администраторы довольно часто встречаются с такой ситуацией. При выходе из строя одного из дисков принимается решение об эксплуатации системы с одним из оставшихся. При этом предполагается, что поскольку этот диск — зеркальная копия, то никаких дополнительных мер предпринимать не надо — достаточно просто загрузить компьютер. Вот тут-то и подстерегает одно НО, о которое спотыкается большинство из тех, кто так попробовал сделать. Если данный раздел диска не является активным, загрузка с него невозможна.

Для активизации раздела воспользуйтесь либо утилитой **FDISK** любой версии MS-DOS (для разделов FAT), либо **Disk Administrator**.

Чередование дисков с записью кода коррекции

RAID 2 работает так, что при записи на диск блок данных разбивается на несколько частей, каждая из которых записывается на отдельный диск. Одновременно создается код коррекции, который также записывается на разные диски. В случае потери данные можно восстановить по коду коррекции с помощью специального математического алгоритма.

Этот метод требует на диске больше места для хранения кода коррекции, чем хранение информации о четности. В Windows NT Server он не используется.

Чередование дисков с записью кода коррекции в виде четности

RAID 3 аналогичен уровню 2 за тем исключением, что код коррекции заменен информацией о четности, записываемой на один диск. Дисковое пространство используется лучше, чем при уровне 2. В Windows NT Server не применяется.

Чередование дисков большими блоками. Хранение четности на одном диске

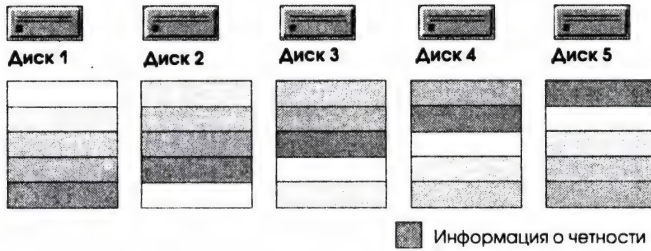
RAID 4 записывает целые блоки данных на каждый диск в массиве. Отдельный диск используется для хранения информации о четности. Всякий раз при записи блока информация о четности должна быть считана, изменена, а затем записана вновь. Этот метод больше годится для операций записи больших блоков, чем для обработки транзакций. В Windows NT Server не применяется.

Чередование дисков с записью информации о четности на все диски

RAID 5 применяется в большинстве современных отказоустойчивых систем. От остальных уровней он отличается тем, что информация о четности записывается на все диски массива. При этом данные и соответствующая им информация о четности всегда располагаются на разных дисках. Если один из дисков выходит из строя, оставшейся информации достаточно для полного восстановления данных.

Чередование дисков с четностью обеспечивает наивысшую производительность для операций чтения. Но при выходе из строя диска скорость чтения резко снижается, поскольку нужно выполнять восстановление данных. Операции записи требуют в три раза больше памяти в сравнении с обычной записью за счет циркуляции информации о четности.

Этот механизм поддерживает от 3 до 32 дисков. Все разделы, кроме загрузочного (системного), могут входить в набор чередования.



Уровень 5 — чередование диска с четностью.

Замена секторов в “горячем режиме”

В Windows NT Server имеется возможность восстановления секторов в процессе работы. При форматировании тома файловая система проверяет все сектора и, обнаружив дефектные, помечает их для исключения из дальнейшей работы. Если плохой сектор обнаружен в процессе записи/чтения, отказоустойчивый драйвер пытается перенести данные в другой сектор, а этот отметить как сбойный. Если перенос удастся, файловая система не предупреждает о проблеме. Эта процедура возможна только на дисках SCSI.

Замена секторов не поддерживается на разделах HPFS.

1. Определяет сбойный сектор

3. Помечает сбойный сектор



2. Перемещает данные в хороший сектор

Замена секторов.

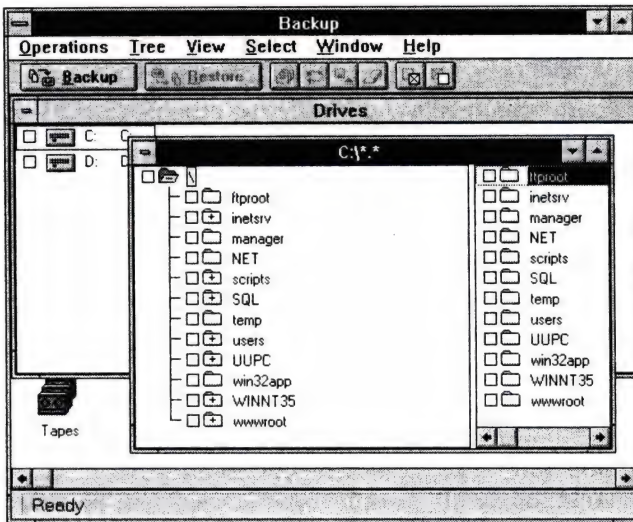
Резервное копирование на магнитную ленту

Windows NT обладает встроенной программой резервного копирования на магнитную ленту (стример). В настоящее время существуют продукты сторонних фирм, обеспечивающие более развитые возможности резервного копирования.

Встроенная поддержка

Windows NT Backup позволяет пользователям выполнять резервное копирование и восстановление данных на локальный накопитель на магнитной ленте (стример). Значок, соответствующий программе резервного копирования, появляется в группе **Administrative Tools** только при наличии в системе стримера. Эту программу можно использовать для:

- резервного копирования и восстановления данных, расположенных на разделах NTFS, FAT и HPFS как на локальном, так и на удаленном компьютере;
- выбора отдельных томов, каталогов или файлов подлежащих копированию/восстановлению. Также можно просматривать подробную информацию о файлах;
- выбора дополнительной проверки, определяющей правильность записи/восстановления;
- выполнения обычных операций резервного копирования: **Normal** (Нормальное), **Copy** (Копирование), **Incremental** (Приращение), **Differential** (Разница) и **Daily** (Ежедневно);
- размещения на одной ленте несколько записей и либо их объединения, либо замещения одной другою;
- выполнения резервного копирования на несколько лент. Таким образом, отсутствует ограничение на размер;
- создания командного файла для автоматизации процесса резервного копирования;
- просмотра полного каталога резервных копий и выбора файлов и каталогов, подлежащих восстановлению;
- выбора диска назначения и каталога, в который будет выполняться восстановление;
- сохранения информации об операциях с лентой в журнале и последующего ее просмотра в **Event Viewer**.



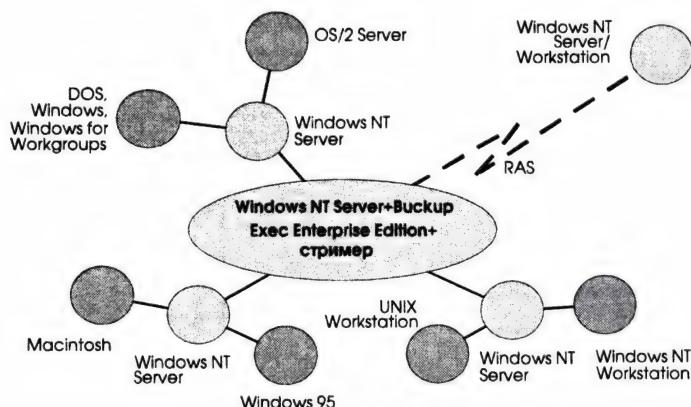
Программа резервного копирования на магнитную ленту.

Продукты сторонних фирм

Кроме встроенной в Windows NT Server утилиты резервного копирования, существует много программ сторонних фирм. Стоит отметить Backup Exec фирмы Arcada, Arcserve фирмы Cheyenne и Backup Director, выпускаемый Palindrome Corp. Все они являются 32-битными приложениями для Windows NT, имеют графический интерфейс и поддерживают идеологию работы по методу “укажи и щелкни”. В то же время они предоставляют ряд дополнительных по сравнению с базовой утилитой возможностей.

Arcada Backup Exec

На основе этого продукта создана утилита Backup Exec, включенная в Windows NT Server. Она работает по принципу клиент-сервер и обладает как центральной административной консолью, так и консолью мониторинга ExecView™, позволяющими управлять несколькими серверами и клиентами одновременно с любой из машин в сети. Удаленное администрирование выполняется с той же производительностью, что и администрирование из центрального узла. Администрирование и мониторинг удаленных клиентов и серверов выполняются с помощью механизма удаленного доступа (RAS) Windows NT, что обеспечивает защиту всей сети. Backup Exec, будучи сервисом Windows NT, обеспечивает высокую степень надежности. Встроенная возможность планирования резервного копирования позволяет выполнять резервное копирование дисков рабочих станций, даже когда никто не зарегистрирован.



Backup Exec интегрирован с продуктами семейства BackOffice. Так, пользователи SQL Server 6.0 могут управлять резервным копированием всей базы данных, журналов транзакций и пр. Пользователи Exchange имеют возможность прозрачного резервного копирования почтовых серверов даже во время их работы. SMS позволяет управлять распространением программного обеспечения, лицензированием и сетевыми операциями, а SNA Server позволяет выполнять резервное копирование на ленточные устройства мэйнфреймов.

Backup Exec поддерживает следующие форматы хранения данных: Microsoft Tape Format (чтение и запись), Cheyenne ARCserve for Netware v4.x и 5.x (только чтение), SyTOS Plus for OS/2 (только чтение) и Maynard Tape Format (только чтение). Поддержка формата Microsoft обеспечивает простоту перехода на эту программу резервного копирования.

Cheyenne ARCserve®

Программа ARCserve, предоставляя практически те же возможности, что и Backup Exec, дополнительно позволяет сообщать информацию администратору или оператору резервного копирования на пэйджер, по электронной почте, в очереди на печать и с использованием SNMP. Еще одно преимущество — возможность резервного копирования/восстановления файлов одновременно на нескольких устройствах, что повышает общую производительность. При восстановлении файлов можно указать дерево каталогов, отдельный каталог, отдельные файлы или сделать запрос.

ARCserve поддерживает только формат ARCserve for Netware v4.x и 5.x.

Palindrome Backup Director Windows NT Edition v.4.0

Этот продукт, аналогичный описанным выше, позволяет выполнять резервное копирование и восстановление файлов на таких клиентах, как Windows, DOS, OS/2 и Macintosh встроенными средствами. Однако для этого требуется сервер Netware. В поставку включен сервер на 100 подключений, что делает возможным резервное копирование только для 100 клиентов.

Положительной стороной является поддержка стримеров, не расположенных на сервере, для чего предназначена встроенная утилита Off-Site Media Advisor.

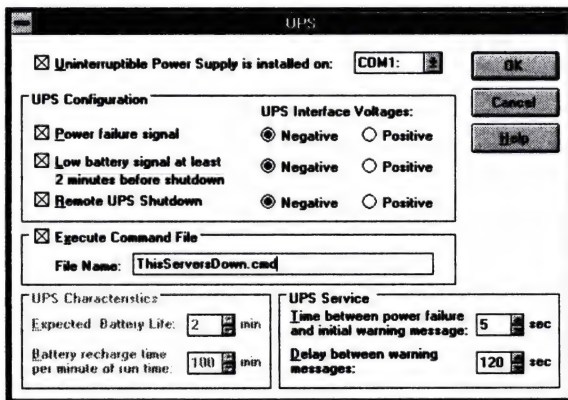
Обеспечение бесперебойного питания

Источники бесперебойного питания (UPS) поддерживают работоспособность системы при сбоях питания за счет энергии аккумуляторных батарей. В Windows NT встроен сервис **UPS**, позволяющий выполнять определенные действия в системе при поступлении сигналов от источника бесперебойного питания. Кроме встроенного сервиса, сторонние производители UPS предлагают дополнительные продукты, обеспечивающие большую функциональность.

Встроенная поддержка UPS

Сервис **UPS** Windows NT определяет свои напряжения питания, предупреждает о них пользователя и корректно заглушает систему при истощении источника резервного питания.

Для настройки параметров этого сервиса предназначен раздел **UPS** в панели управления.



Диалоговое окно настройки параметров UPS.

К настраиваемым параметрам относятся:

- последовательный порт, к которому подключен источник бесперебойного питания;
- наличие сигнала от UPS при сбое напряжения питания;
- наличие предупреждения от UPS при снижении уровня зарядки батарей;
- наличие сигнала от сервиса UPS для выключения источника бесперебойного питания;
- командный файл, выполняемый перед выключением компьютера;
- ожидаемое время работы и перезарядки батарей;
- временные интервалы для предупреждающих сообщений.

Сервис **UPS** должен использоваться совместно с сервисами **Alerter**, **Messenger** и журналом регистрации. При этом все события, связанные с сервисом **UPS** (например, сбой питания или сбой подключения источника бесперебойного питания), будут занесены в журнал регистрации, а определенные пользователи получат о них уведомления по сети. С помощью опции **Server** на панели управления можно назначить пользователей и/или компьютеры, которые будут получать эти уведомления.

Продукты сторонних фирм

Стоит отметить разработки фирмы APC — PowerChute и PowerChute plus. Эти продукты позволяют выполнять автоматическую перезагрузку и выключение компьютера, уведомлять пользователя о сбоях питания с помощью сигналов тревоги и по электронной почте, а также отображать на экране в реальном масштабе времени текущее состояние источника бесперебойного питания (напряжение, температуру, уровень зарядки батарей и т.п.). PowerChute предоставляет возможность выполнять проверки UPS в автоматическом режиме и заносить в журнал все события, связанные с работой UPS.

Контролировать работу UPS на разных серверах можно с одной рабочей станции, при этом для обеспечения защиты необходим пароль. Администратор может также указать, как реагировать на каждое из возможных событий.

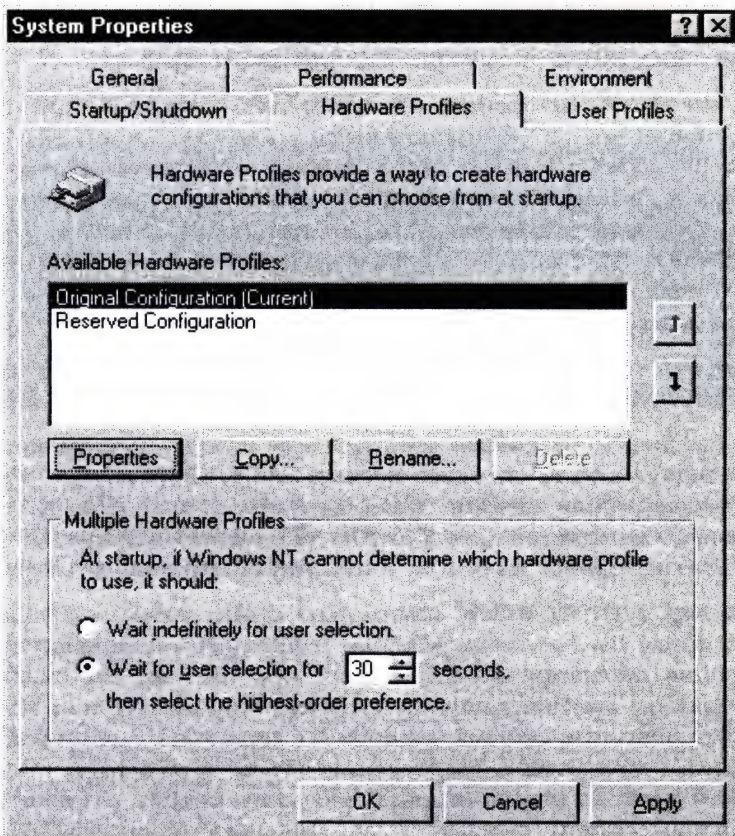
Выбор работоспособной конфигурации

В процессе загрузки системы имеется возможность выбора последней работоспособной конфигурации (**Last Known Good Configuration**). Она позволяет отказаться от модификаций, внесенных в конфигурацию системы. Например, в предыдущем сеансе работы Вы указали неверный тип видеоадаптера. Для восстановления работоспособности системы достаточно выбрать **Last Known Good Configuration**, когда система предложит это сделать.

Выбор профиля техники

4.0

В версии Windows NT 4.0 появилась возможность определения профиля техники, который будет использоваться системой. Это удобно на мобильных компьютерах, способных функционировать как “сами по себе”, так и будучи подключенными к материнским блокам (docking station). Однако, конфигурируя такой профиль, можно указать, например, на загрузку системы с полностью отключенными сетевыми функциями, что иногда бывает весьма полезно. Для создания профиля в утилите **System** выберите вкладку **Hardware Profiles** в панели управления.



Диалоговое окно *System Properties*.

Как только Вы создадите хотя бы один дополнительный профиль, он будет предлагаться в качестве альтернативы при загрузке системы. В случае Вашего отсутствия будет выбран профиль по умолчанию.

Emergency Repair Disk

Emergency Repair Disk позволяет пользователю восстановить систему в то состояние, в каком она была сразу после установки. Этот диск используется, когда системные файлы повреждены и пользователь не может восстановить систему вызовом последней работоспособной конфигурации. Диск **Emergency Repair Disk** создается во время установки Windows NT. В дальнейшем его можно создать командой **RDISK**, однако такой диск не позволит восстановить систему в первоначальное состояние.

Emergency Repair Disk выполняет следующие функции:

- Сверяет дерево каталога Windows NT с тем, что записано в журнале, и проверяет целостность и наличие всех системных файлов.

Если какой-либо из файлов пропущен или поврежден, происходит его восстановление с соответствующей дискеты или CD-ROM-диска с Windows NT. На компьютерах с процессорами x86 пользователю предлагается вставить дискеты или CD-ROM-диск, с которых выполнялась установка. Если установка выполнялась с помощью программы **WINNT.EXE**, для восстановления потребуется тот комплект дискет или тот компакт-диск, с которого создавался сетевой каталог, из которого выполнялась установка.

- Проверяет файлы Windows NT в системном разделе и определяет наличие и целостность всех файлов.

Если какой-либо из файлов пропущен или поврежден, его восстановление происходит с соответствующей дискеты или CD-ROM-диска с Windows NT. Если пользователь случайно переформатировал или изменил системный раздел на компьютере с процессором x86, так что Windows NT больше не стартует, программа восстановит начальную загрузочную конфигурацию.

Например, если на Вашем компьютере стояла только система Windows NT, а потом Вы поставили MS-DOS, Windows NT перестанет загружаться. Выполнив процедуру восстановления, при загрузке Вы сможете выбрать одну из двух операционных систем: Windows NT или MS-DOS. Еще пример. Допустим, система Windows NT установлена на второй физический диск в компьютере, а загрузочные файлы — на первом. После замены первого диска на новый, например большего объема, для восстановления работоспособности системы лишь выполните процедуру восстановления с Emergency Repair Disk.

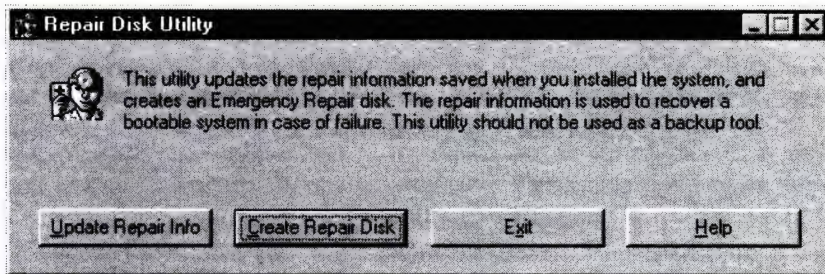
Если установка выполнялась не с дискет и не с CD-ROM-диска, а с помощью программы **WINNT.EXE**, для восстановления потребуется тот комплект дискет или тот компакт-диск, с какого создавался сетевой каталог, из которого выполнялась установка.

- Проверяет наличие ошибок в реестре. Если обнаруживаются поврежденные файлы, пользователю предоставляется возможность их восстано-

ния с помощью **Emergency Repair Disk**. При этом восстанавливаются бюджеты пользователей и защита файлов, существовавшие на момент создания **Emergency Repair Disk**. Для этого выполняется резервное копирование каталога `\winnt35\system32\config`.

- Снимает защиту с системных файлов, если Windows NT установлен на разделе NTFS. Это пригодится, если пользователь случайно установит такие права доступа к системным файлам, что система не сможет получить доступа к необходимым для запуска файлам.

Советую регулярно создавать новые копии **Emergency Repair Disk** командой **RDISK**. Это особенно актуально после выполнения обновлений системы с помощью так называемых сервисных пакетов (Service Packs). Страховочный диск, созданный после установки сервисного пакета, избавит Вас в дальнейшем от процедуры переустановки сервисного пакета после восстановления исходного состояния системы.



Утилита **RDISK**.

Утилита **RDISK** имеет графический интерфейс и позволит либо создать новый страховочный диск (**Create Repair Disk**), либо обновить информацию на уже имеющемся (**Update Repair Info**).

Зеркализация серверов

Описанные выше способы обеспечения надежного хранения данных можно использовать, только когда сам сервер работает надежно. В случае краха сервера его клиенты будут на какое-то время лишены возможности доступа к данным. И это продлится тем дольше, чем больше потребуется времени администратору на восстановление самого сервера либо данных с ленты на другом сервере. Так что возникает необходимость резервирования информации в реальном масштабе времени.

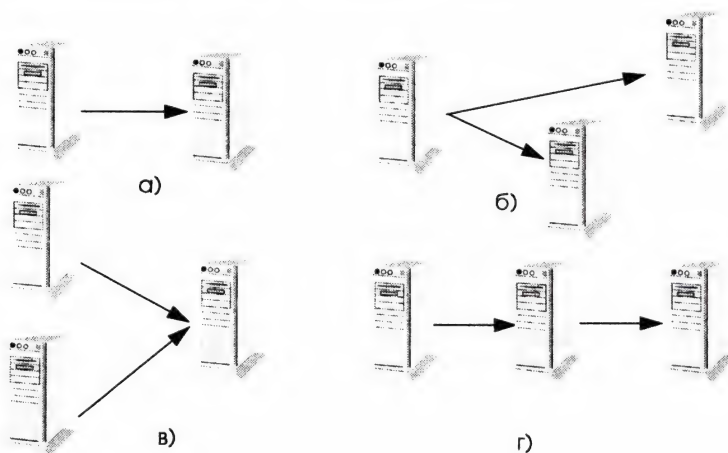
Фирма Novell разработала продукт SFT III, позволяющий это делать для Netware. В Windows NT такая функция не встроена. Казалось бы, можно использовать службу тиражирования каталогов, но она действует не в реаль-

ном масштабе времени и предназначена только для предоставления распределенного доступа к специфичной информации.

Фирмой Octopus Technologies Inc. выпускается Octopus Real Time Data Protection. С помощью этого продукта можно организовать зеркализацию файлов или каталогов с одного сервера на один или несколько других серверов или рабочих станций.

В Octopus связь между серверами основана на вызовах удаленных процедур. Информацией, посылаемой в зеркальные каталоги, является только обновление файлов и каталогов. Например, если использовать Octopus для резервирования базы данных, по сети реально передаются только обновления (удаленные или добавленные записи). Если бы каждый раз передавалась вся база, это привело бы к резкому возрастанию трафика в сети и снижению ее производительности.

Еще один плюс Octopus: серверы связаны обычной сетью, и при этом не требуется особый протокол. Достаточно установить серверную часть на компьютер, данные которого должны резервироваться, и клиентскую часть — на компьютеры, куда будут поступать данные. Возможны следующие комбинации резервирования: с одного сервера на другой, с одного на несколько других, с нескольких на несколько и с нескольких на один. Обновления файлов выполняются на транзакционном уровне. Транзакция всегда должна быть завершена, иначе происходит откат.



Варианты зеркализации серверов в системе Octopus: а) один в один; б) один в несколько; в) несколько в один; г) цепью.

А что произойдет в случае краха сервера при использовании системы Ostorus? Все зависит от версии. В стандартной версии администратор системы должен либо восстановить исходный сервер, либо переключить всех пользователей на тот, что был зеркальным. Последние версии Ostorus имеют дополнительную функцию автоматического переключения (Automatic Switching Option), позволяющую автоматически переключать пользователей на зеркальный сервер при крахе основного. В любом случае самые последние версии файлов останутся сохраненными.

Несмотря на простоту и относительно невысокую стоимость, у такой системы есть один минус: пользователям необходимо переключаться на новый сервер, перезапускать процессы и заново открывать файлы. К тому же при этом теряется и содержимое оперативной памяти.

Кластеры серверов

Высшая надежность достигается с помощью кластерных систем, обеспечивающих не только надежность хранения данных, но и непрерывность процессов, выполняющихся в кластере, а также производительность, определяемую совокупностью всех серверов, входящих в кластер.

Совсем недавно кластерных систем для Windows NT не существовало. Однако в последнее время ряд компаний (AT&T Global Information Solutions, Compaq Computer Corp., Digital Equipment Corp., Hewlett-Packard и Tandem Computers Inc.) предложил варианты кластерных решений для Windows NT.

Определение кластеров

В общем случае кластером называется группа независимых систем, работающих как единое целое. Клиент взаимодействует с кластером как с одним сервером. Кластеры используются как для повышения доступности, так и для наращиваемости.

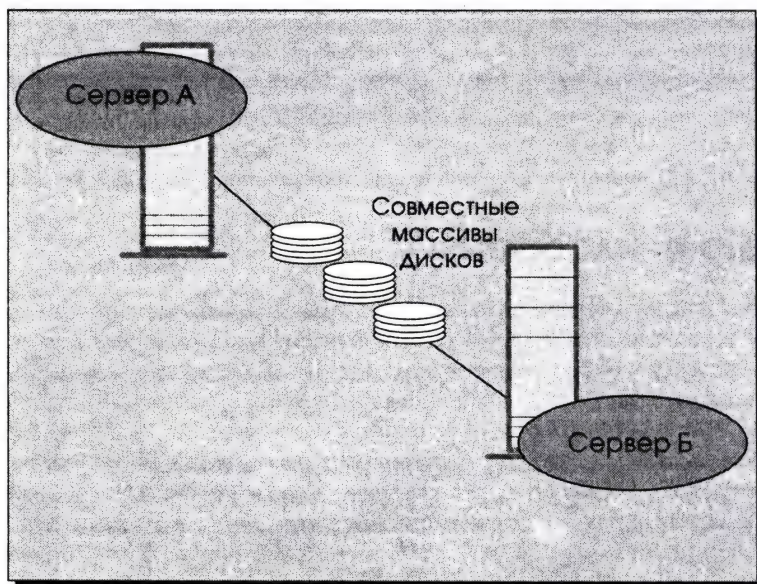
Доступность: Когда одна из систем, составляющих кластер, выходит из строя, программное обеспечение кластера распределяет работу, выполнявшуюся ею, между другими системами кластера.

Наращиваемость: Когда общая нагрузка системы достигает предела возможностей систем, составляющих кластер, его можно нарастить, добавив дополнительную систему. Раньше для этого мы вынуждены были приобретать дорогостоящие компьютеры, позволяющие устанавливать дополнительные процессоры, диски и память. А с помощью кластеров Вы увеличите производительность по мере необходимости, просто добавляя новые системы.

Иллюстрация кластеров — доступность данных

В качестве примера рассмотрим работу современного супермаркета. Его расчетные центры — сердце бизнеса. Кассовые аппараты должны быть постоянно подключены к базе данных магазина, хранящей информацию о продуктах, кодах, названиях и ценах. Если связь рвется, теряется возможность обслуживания клиентов, падает прибыль, и, что, может быть, хуже всего, — подрывается репутация фирмы.

В этом случае кластерная технология используется для повышения доступности системы. В нашем примере можно предложить использование двух систем, подключенных к многопортовому дисковому массиву, на котором располагается база данных. В случае сбоя сервера А резервная система (сервер Б) автоматически подхватит соединение так, что пользователи и не заметят, что произошел сбой. Таким образом, комбинируя технологию обеспечения повышенной надежности работы с диском, стандартно используемую в Windows NT Server 3.51 (чередование, дублирование и т.д.), с кластерной технологией, обеспечивают гарантированное обеспечение доступности системы.



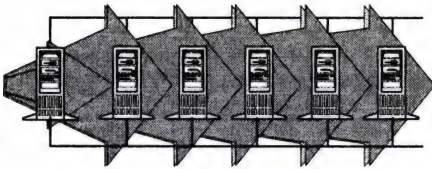
Обеспечение непрерывного доступа.

Иллюстрация кластеров — наращиваемость

В качестве примера наращиваемости рассмотрим финансовый бизнес. Всю полноту ответственности за работу финансовой или банковской системы, естественно, несет главный технический специалист. Он отлично понимает, что малейший сбой системы повлечет за собой колоссальные финансовые потери и град упреков в его адрес. С другой стороны, безукоризненная работа системы в конечном итоге приведет к тому, что на нее будет перекладываться все больше и больше задач. Все это приведет к истощению возможностей системы и необходимости разработки и создания новой.

Эти соображения приводили до недавнего времени к тому, что технические специалисты банков вынуждены были сразу закладывать на потенциально колоссальные вычислительные потребности и создавали системы на базе больших мэйнфреймов и мини-ЭВМ.

Кластерная технология на базе Windows NT Server предоставляет потрясающую возможность — отказаться от дорогостоящего оборудования и использовать широко распространенную систему на самых обычных аппаратных платформах. Наращивание мощности достигается простым добавлением еще одной системы в кластер.



Наращивание суммарной мощности кластера при включении в него дополнительных систем.

Традиционная архитектура предоставления высокой доступности

Сегодня повышение доступности компьютерных систем достигается несколькими способами. Самый типичный — дублирование систем с полностью тиражируемыми компонентами. Программное обеспечение такой системы постоянно отслеживает состояние работающей системы, а вторая система все это время простаивает. В случае сбоя первой происходит переключение на вторую. Такой подход, с одной стороны, значительно повышает стоимость оборудования без повышения производительности системы в целом, а с другой — не обеспечивает защиты от ошибок в приложениях.

Традиционная архитектура обеспечения наращиваемости

Наращиваемость сегодня также обеспечивается несколькими способами. Создать систему с наращиваемой производительностью можно, например, используя симметричную мультипроцессорную обработку (SMP). В SMP-системах несколько процессоров используют одну общую память и устройства ввода/вывода. В традиционной модели "совместного использования памяти" выполняется одна копия операционной системы, а процессы прикладных задач работают так, будто в системе лишь один процессор. При запуске в такой системе приложений, не использующих общие данные, достигается высокая степень наращиваемости.

Основным тормозящим фактором использования систем с симметричной обработкой являются физические ограничения скорости работы шины и доступа к памяти. По мере увеличения скорости работы процессоров возрастает их стоимость. Сегодня пользователь, возжелавший добавить 2-4 процессора (а в особенности более 8), должен заплатить бешенные деньги, совершенно непропорциональные числу процессоров.

Архитектура кластера

Кластеры могут иметь разные формы. Например, в качестве кластера может выступать несколько компьютеров, связанных по сети Ethernet. Кластерами высокого уровня являются высокопроизводительные многопроцессорные SMP-системы, связанные высокоскоростной шиной, связи и ввода-вывода. В обоих случаях увеличение вычислительной мощности достигается небольшими шагами при добавлении очередной системы. С точки зрения клиента, кластер представляется в виде одного сервера или *образа одной системы*, хотя реально состоит из нескольких компьютеров.

Сегодня в кластерах используются в основном две модели: *с общими дисками* и *без общих компонентов*.

Модель с общими дисками

В модели с общими дисками программное обеспечение, исполняемое на любой из систем, входящих в кластер, имеет доступ к ресурсам систем кластера. Если двум системам нужны одни и те же данные, то они либо дважды считываются с диска, либо копируются с одной системы на другую. В SMP-системах при-

ложение должно синхронизировать и превратить в последовательный вид доступ к общим данным. Обычно для организации синхронизации используется Диспетчер распределенных блокировок (***Distributed Lock Manager*** — DLM). Сервис DLM позволяет приложениям отслеживать обращения к ресурсам кластера. Если к одному ресурсу обращается более двух систем одновременно, Диспетчер распределенных блокировок распознает и предотвращает потенциальный конфликт. Процессы DLM могут приводить к дополнительному трафику сообщений в сети и снизить производительность. Один из способов избежать этого эффекта — программная модель *без общих компонентов*.

Модель без общих компонентов

В модели без общих компонентов каждая система, входящая в кластер, владеет подмножеством ресурсов кластера. В каждый момент времени только одна система имеет доступ к определенному ресурсу, хотя при сбоях другая динамически определяемая система может вступить во владение этим ресурсом. Запросы от клиентов автоматически перенаправляются к тем системам, что владеют необходимым ресурсом.

Например, если в запросе клиента содержится обращение к ресурсам, находящимся во владении нескольких систем, одна система выбирается для обслуживания запросов (ее называют хост-система). Затем эта система анализирует запрос и передает под запросы соответствующим системам. Они выполняют полученную часть запроса и результат возвращают хост-системе, которая формирует окончательный результат и отправляет его клиенту.

Одиночный системный запрос к хост-системе описывает высокоуровневую функцию, порождающую системную активность, а внутрикластерный трафик не генерируется до тех пор, пока не будет сформирован конечный результат. Приложение, распределенное между несколькими системами, входящими в кластер, позволяет преодолеть технические ограничения, присущие одному компьютеру.

Модели с общим диском и модель без общих компонентов могут работать в пределах одного кластера. Некоторые программы наиболее просто используют возможности кластера в рамках модели с общим диском. К таким приложениям относятся задачи, требующие интенсивного доступа к данным, а также задачи, которые трудно разделить на части. Приложения, для которых важна наращиваемость, должны использовать модель без общих компонентов.

Серверы кластерных приложений

В то время как кластеры предоставляют доступность и наращиваемость для всех серверных приложений, специальные "кластерные" приложения могут использовать все преимущества кластеров. Серверы баз данных должны быть улучшены за счет добавления либо функций координации доступа к общим данным в кластерах с общим диском, либо функций разделения запросов на более простые запросы в кластерах без общих компонентов. В таких кластерах сервер баз данных сможет задействовать все преимущества разделения данных путем выполнения параллельных запросов. Дополнительно к этому серверные приложения могут быть расширены функциями автоматического определения неработающих компонентов и инициации быстрого восстановления.

Исторически для создания кластерных приложений использовались Мониторы обработки транзакций. Монитор транзакций отвечает за перенаправление клиентских запросов к соответствующим серверам внутри кластера, распределения запросов между серверами и координации транзакций между серверами кластера. Монитор транзакций также может заниматься балансировкой нагрузки, автоматическим переключением и повторением исполнения запроса в случае сбоя на сервере, а также принимать участие в процессе восстановления после сбоев.

Кластеры на основе Windows NT Server

Сервер Windows NT Server 3.51 содержит базовые компоненты, необходимые для построения кластеров. К ним относятся, например, возможность однократной регистрации, унаследованная из доменной архитектуры сети, возможность всех административных утилит выполнять мониторинг нескольких систем, а также возможность перенаправлять запросы через редиректор.

Кластерные расширения представляют целый спектр технологий, которые будут реализованы с течением времени. При реализации этих расширений будут расставлены приоритеты, основанные на требованиях клиентов.

Двухфазный подход

В настоящее время Microsoft разрабатывает интерфейс программирования кластеров (Cluster Application Programming Interfaces — CAPI), который позволит приложениям воспользоваться преимуществами Windows NT Server в кластере.

Разработка кластеров разбивается на 2 фазы:

Фаза 1: Защита от сбоев

Данное решение позволяет повысить доступность данных путем предоставления возможности двум серверам использовать одни и те же жесткие диски внутри кластера. В случае сбоя одного сервера, управление и задачи им выполняемые передаются на второй так, что в большинстве случаев сбой проходит незамеченным для приложения.

Фаза 2: Нарастиваемое решение

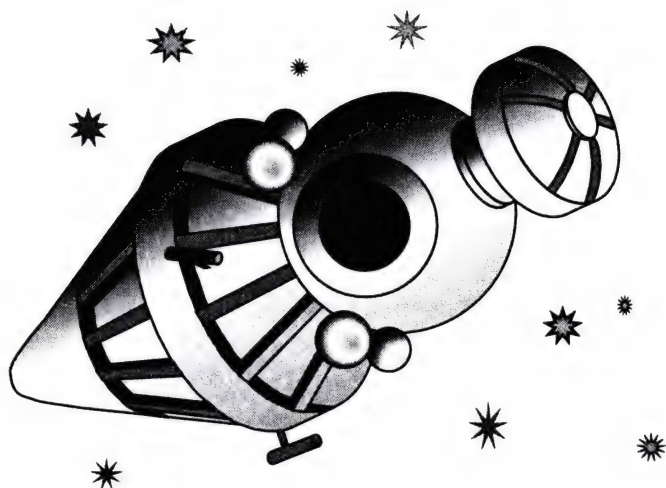
В терминах нарастиваемости общая производительность кластера определяется совокупной производительностью систем, составляющих кластер. Пользователю предоставляется возможность повышать мощность не путем приобретения дорогостоящих многопроцессорных компьютеров, а добавляя новые относительно дешевые системы.

Конструкция предполагает возможность использования в кластере нескольких узлов, однако на первых порах будет введена поддержка только двух узлов. Независимо от платформы, на которой исполняется Windows NT (x86, MIPS, ALPHA, PPC), системы будут доступны для объединения.

Кластерные расширения будут встроены не только в сам сервер, но и в продукты BackOffice (например, SQL Server и Exchange Server).

Разграничение доступа к принтерам

Чем больше пользователей нуждается в выводе на печать своих документов, тем выше вероятность того, что все они захотят сделать это одновременно. Задача администратора — сделать так, чтобы не возникло конфликтных ситуаций, плюс к тому обеспечить невозможность для “непосвященных” случайно подглядеть конфиденциальные документы. Механизмы управления печатью в Windows NT Server чрезвычайно просты и удобны в работе.



Работа с принтерами

Для управления и администрирования принтерами предназначены **Print Manager** и **Server Manager**. Эти операции доступны пользователям, входящим в группы **Administrators**, **Server Operators** или **Print Operators**. Если пользователь не входит ни в одну из перечисленных групп, его доступ к принтеру определяется членом одной из них.

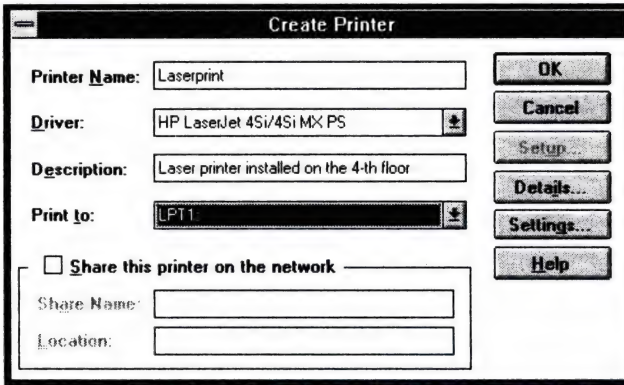
Print Manager доступен через панель управления **Control Panel** и позволяет авторизированным пользователям:

- > добавлять и удалять принтеры;
- > конфигурировать принтеры;
- > печатать на принтер или в файл;
- > предоставлять принтер в совместное использование в сети;
- > определять время, в течение которого к принтеру открыт доступ;
- > управлять заданиями на печать, посланными на принтер;
- > просматривать принтеры, находящиеся в сети, и находить незагруженные;
- > останавливать и возобновлять печать;
- > устанавливать порядок печати в очереди на печать;
- > управлять локальными и удаленными принтерами;
- > удалять задания из очереди на печать;
- > устанавливать часы, в течение которых принтер доступен;
- > управлять типом доступа к принтеру.

Создание принтера

Под созданием принтера подразумевается установка в системе соответствующего драйвера. Физически принтер может быть подключен как локально (к параллельному и последовательному порту), так и по сети — с использованием протоколов TCP/IP или DLC. К одному серверу можно подключить неограниченное число принтеров.

Для создания принтера в **Print Manager** в меню **Printer** выберите команду **Create**, а затем в списке диалогового окна **Create Printer** — соответствующий тип принтера. Принтеру необходимо дать имя, например Laserprint.



Диалоговое окно *Create Printer*.

4.0

В Windows NT 4.0 процедура создания нового принтера существенно изменилась. Связано это не только с тем, что теперь она более ориентирована на пользователя, но и с тем, что изменился сам механизм печати. Новая версия использует Enhanced Metafiles (EMF), что заметно ускоряет печать. Кроме ускорения, появляется возможность печати одного и того же файла EMF на любом принтере.

Для создания нового принтера необходимо использовать Мастер создания принтеров (*Add Printer Wizard*), размещающийся в папке *My Computer*. На рисунке показаны некоторые из шагов, которые необходимо сделать в целях добавления в систему нового принтера.

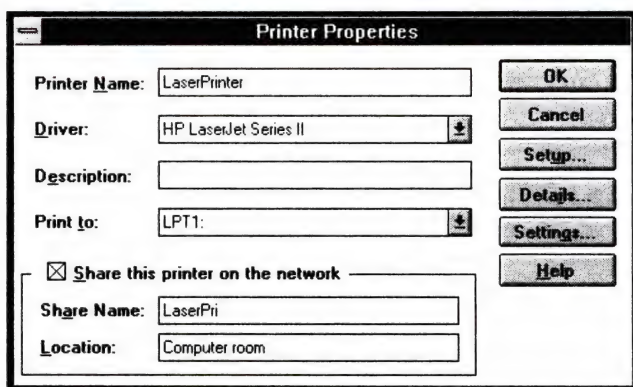


Окна Мастера добавления нового принтера.

- При подключении к сетевому принтеру, управляемому Windows NT версии 4.0, Вам не понадобится устанавливать сам драйвер принтера, так как
- будет использоваться тот, что установлен на сервере. В случае использования любого другого принтера (даже управляемого Windows NT 3.5x)
- установка драйвера обязательна.

Совместное использование принтеров

Чтобы предоставить принтер в совместное использование, в **Print Manager** выберите необходимый принтер, в диалоговом окне **Printer Properties** укажите имя принтера, под которым он будет доступен в сети, и его положение.



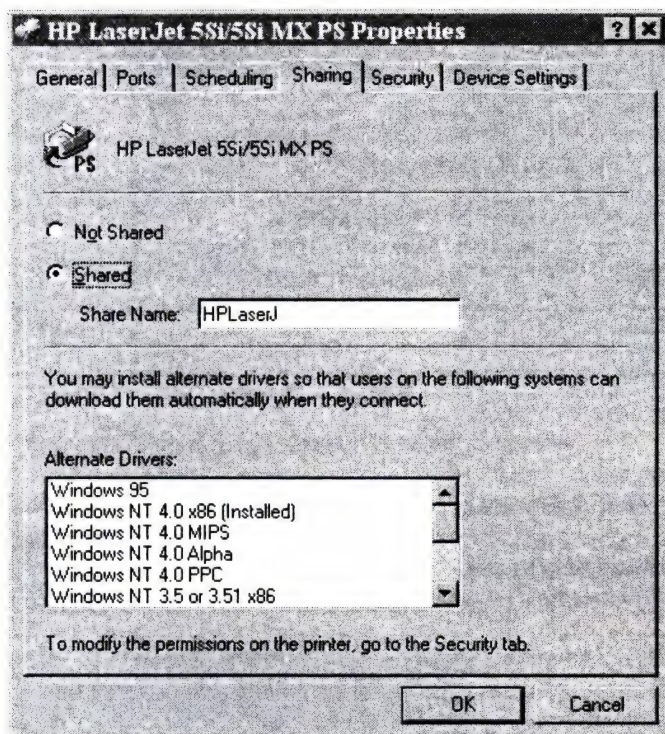
Диалоговое окно *Printer Properties*.

В этом диалоговом окне нельзя указать пользователей или группы, имеющие доступ к принтеру, а также тип доступа. Для этого предназначено диалоговое окно **Printer Permissions**.



- В Windows NT версии 4.0 предоставление принтера в совместное использование позволяет не только выполнять печать с рабочих станций, но и автоматически загружать необходимый для определенного клиента драйвер принтера. Допустим, Вы работаете на компьютере в среде Windows 95. При подключении к сетевому принтеру Вам не потребуется обращаться к заветной коробочке с дистрибутивом системы, чтобы установить драйвер, — будет использоваться тот, что был для Вас заботливо установлен на сервере администратором сети.

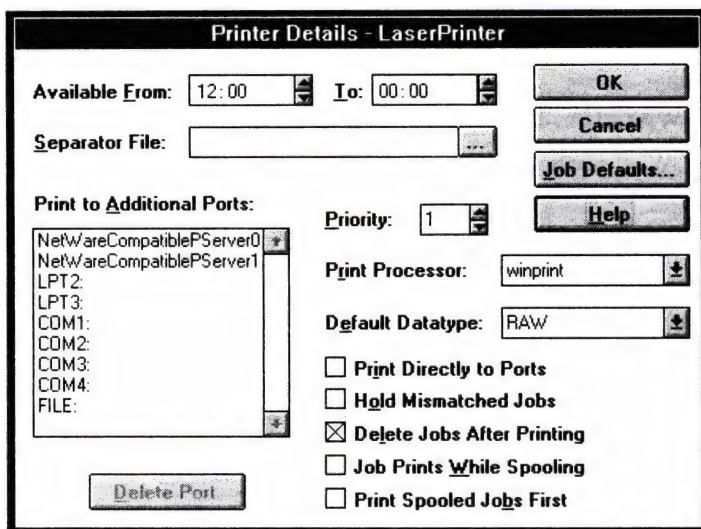
Все, что должен для этого сделать администратор, — указать в списке всех возможных клиентов печати. К поддерживаемым таким образом клиентам относятся Windows 95 и Windows NT версий 3.1, 3.5, 3.51 и 4.0 для всех аппаратных платформ, на которых работает эта система.



Предоставление принтера в совместное использование в Windows NT 4.0.

Настройки принтера

Настройка некоторых параметров принтера доступна через диалоговое окно **Printer Details**. В нем можно определить часы, в течение которых принтер доступен, разделительную страницу, создать пул принтеров, указать приоритет принтеров, процессор печати, тип данных по умолчанию, а также указать на необходимость печати непосредственно в порт. Единственная функция в этом окне, относящаяся к безопасности печати, — определение часов, в течение которых принтер доступен.



Диалоговое окно *Printer Details*.

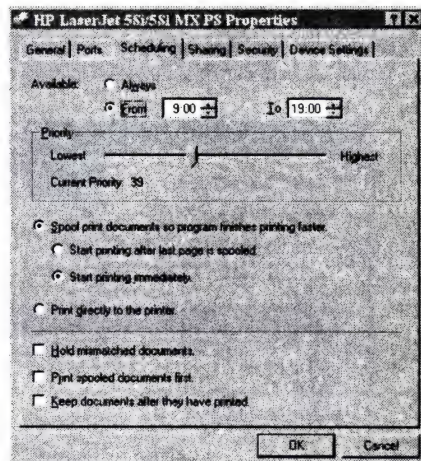
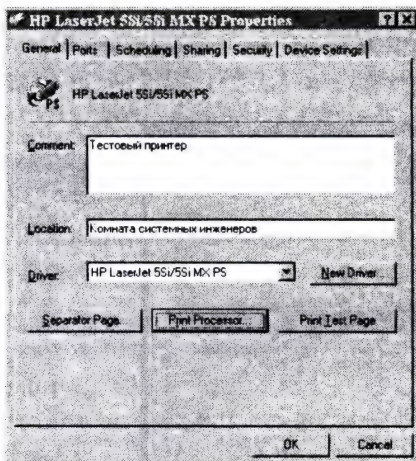
Например, Дима указал, что Laserprinter доступен с 10-00 до 15-00. Если Саша попытается вывести документ на этот принтер в 16-00, документ попадет в очередь на печать, но не будет напечатан. Сашин документ будет находиться в очереди на печать, пока не наступит разрешенное время либо пока Дима не выберет этот документ в очереди и не укажет для него другое доступное время печати.

Если Сашин документ находился в очереди на печать в момент изменения времени доступности принтера, так что оно захватывает текущее время, то все новые документы, попадающие в очередь, будут распечатаны. Но Сашин документ будет в очереди, пока не наступит время, указанное в качестве доступного на момент попадания документа в очередь, либо пока Дима не укажет для этого документа новое время.



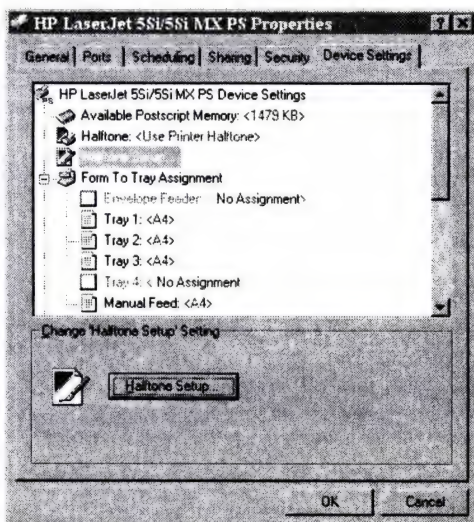
- В Windows NT 4.0 настройки принтера разделены. В диалоговом окне **Printer Properties** есть следующие разделы:
- **General** — описание общих параметров принтера, процессора печати и драйвера;
- **Ports** — список всех используемых для подключения принтеров портов
- **Scheduling** — параметры, определяющие скорость печати и доступность принтера. Также в этом разделе можно указать приоритет печати документов. Интересно, что, указывая на необходимость выполнения спулин-

га при печати, Вы можете выбрать опцию, при которой сам процесс печати начнется сразу, не дожидаясь окончания спулинга.



Страницы диалогового окна *Printer Properties*.

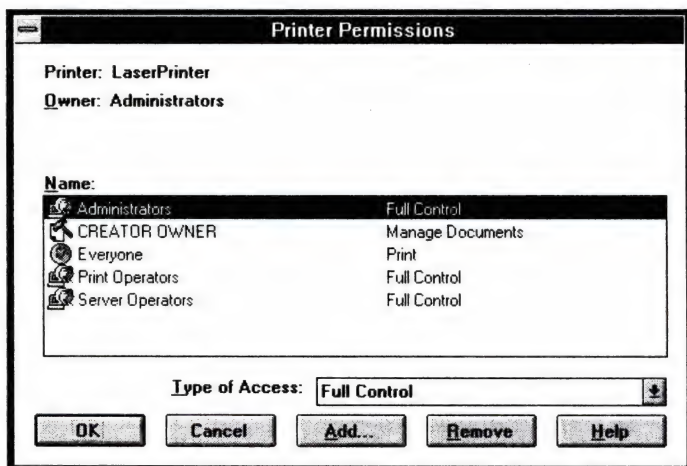
Тонкая настройка остальных параметров принтера выполняется в разделе **Device Settings**. Параметры, специфичные для каждого вида принтера, представлены в виде древовидной структуры. Выбирая тот или иной элемент структуры, Вы получите доступ к элементам настройки параметра.



Окно тонкой настройки параметров принтера.

Права доступа к принтеру

Права доступа к принтеру назначаются при выборе команды **Printer Permissions** в меню **Security**. В появляющемся при этом диалоговом окне укажите пользователей или группы, имеющие доступ к принтеру, а также тип этого доступа.



Диалоговое окно *Printer Permissions*.

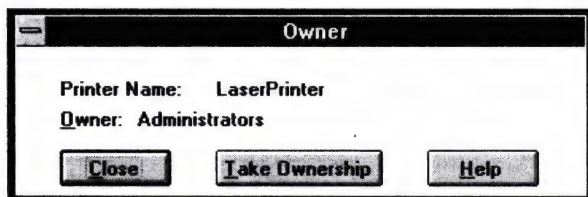
	No Access	Print	Manage Documents	Full Control
Печать документов		•		•
Управлять настройками документов			•	•
Приостанавливать, возобновлять, перезапускать и удалять печать документов			•	•
Изменять порядок печати				•
Приостанавливать, возобновлять и очищать принтер				•
Изменять свойства принтера				•
Удалять принтер				•
Изменять права доступа к принтеру				•

Права доступа кумулятивны, но **No Access** преобладает над остальными.

Все вновь создаваемые пользователи по умолчанию принадлежат к группе **Domain Users** и могут печатать и удалять свои задания на печать, но не управлять документами. Чтобы изменить права доступа к принтеру, пользователю нужно быть либо владельцем принтера, либо иметь полный доступ. Он также может видеть права печати для каждой группы.

Владелец

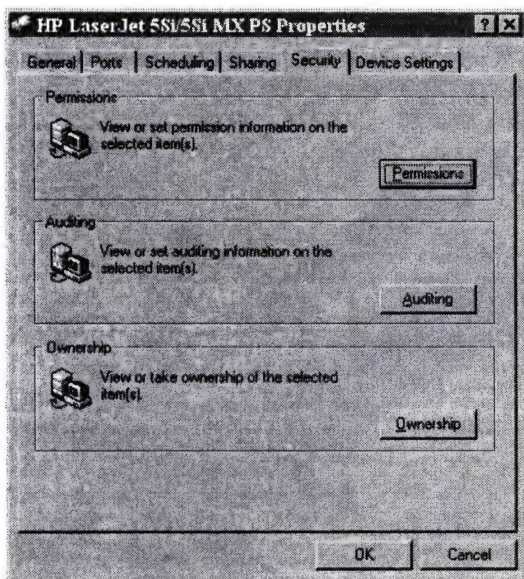
Владелец принтера назначается в меню **Security**. Пользователь, имеющий полный доступ к принтеру или принадлежащий к группе администраторов, может вступить во владение принтером. Владение принтером позволяет изменять права доступа к нему.



Диалоговое окно *Owner*.

4.0

Так как в Windows NT 4.0 отсутствует **Print Manager**, то для разграничения доступа используется описанное ранее диалоговое окно **Printer Properties**, раздел **Security**.



Из этого раздела Вы попадаете в диалоговые окна определения прав доступа, аудита и владельца, “нажимая” соответствующие кнопки. Ничего принципиально нового по сравнению с предыдущей версией в этих параметрах не появилось.

Защита спул-файла

При печати на локальном принтере будет выполняться спулинг задания на диск. Если спул-каталог находится в разделе NTFS, то пользователь, не имеющий прав доступа к нему, не сможет осуществлять печать. По умолчанию группа **Everyone** имеет право доступа **Change** к каталогу спулинга. Если изменяется положение спул-каталога, удостоверьтесь, что все пользователи имеют право доступа **Change** к нему.

Защита реестра

Значения, регулирующие процесс печати, хранятся в реестре в подключе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print. Если администратор через редактор реестра установил для пользователя только право чтения этого ключа, пользователь не установит и не сконфигурирует принтеры, так как **Print Manager** будет не в состоянии изменить этот подключ.

Приложения Windows пытаются найти информацию о доступных принтерах в реестре в подключе HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\PrinterPorts. Если у пользователя нет разрешения записи этого подключа, приложения Windows не распознают вновь добавленные принтеры и могут пытаться обратиться к удаленным принтерам.

Взаимодействие с Novell Netware

Не так давно известные строчки Маяковского можно было смело перефразировать таким образом: “мы говорим — сети, подразумеваем — Netware”. И хотя сегодня это утверждение уже далеко не бесспорно, тысячи сетей используют в качестве основы серверы Novell Netware. Система, предназначенная для сети, но не понимающая Novell, обречена. Windows NT Server “учился” работать с Netware от версии к версии. Посмотрим на результаты этой учебы.



ОСНОВНЫЕ ВИДЫ ВЗАИМОДЕЙСТВИЯ

Пользователи, пришедшие в мир Windows NT из мира Netware, на вопрос, как они представляют себе взаимодействие между этими двумя системами, с ходу ответят, что необходимо:

предоставить пользователям Windows NT доступ к серверам Netware.

Потом, слегка подумав и вспомнив, что на базе Windows NT Server можно строить сети с самыми разнообразными клиентами, выдвинут еще пару требований:

предоставление клиентам сети Microsoft доступа к серверу Netware и

предоставление клиентам сети Netware доступа к ресурсам доменов Windows NT.

Если же они знают, что Windows NT Server — прекрасный сервер приложений, то, несомненно, добавляют:

возможность для клиентов Netware работать с серверными приложениями Windows NT.

Уверен, что после непродолжительных размышлений о тяжелой доле администратора гетерогенной (смешанной) сети, в этот список будет внесена

возможность централизованного управления двумя сетями.

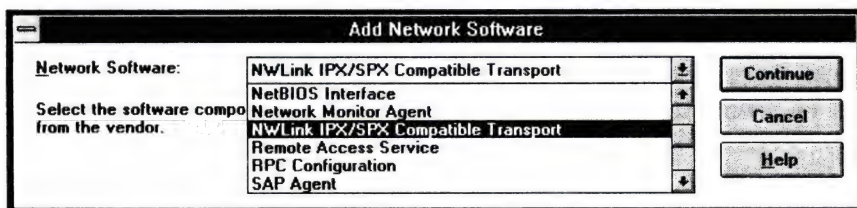
Ну и наконец, тем, кто уже вкусил и того и другого, познал радости и огорчения от двух сетей, припомнил все бессонные ночи, придет в голову совсем уже крамольная мысль о

быстром и безопасном переходе от сети Netware к сети Windows NT Server.

“Не многовато ли будет?!” — воскликнет кое-кто. Отнюдь нет — такими свойствами обладает текущая версия NT Server. О них-то и рассказано в данной главе, так сказать, в “хронологическом порядке” — в той последовательности, в какой появлялись новые возможности взаимодействия в Windows NT.

Доступ к серверным приложениям Windows NT Server

Первые пользователи появившегося в 1993 году Windows NT Advanced Server 3.1 недоуменно пожимали плечами, читая о встроенной в него возможности взаимодействия с Netware. Им было совершенно невдомек, зачем нужен протокол **NWLink IPX/SPX Compatible Transport**.



Добавление протокола NWLink IBX/SPX.

После его добавления как будто ничего не происходило: с NT-компьютера не становились видны серверы Netware, как, впрочем, и ресурсы NT Server — с клиентов Netware.

Ларчик открывается просто: этот вид транспорта нужен только для предоставления доступа к серверным приложениям, выполняемым на сервере NT. Вот если на сервере запустить Microsoft SQL Server, а на клиентах Netware — работающие с ним клиентские приложения, они прекрасно увидят сервер и смогут как посылать на него запросы, так и получать ответы на них.

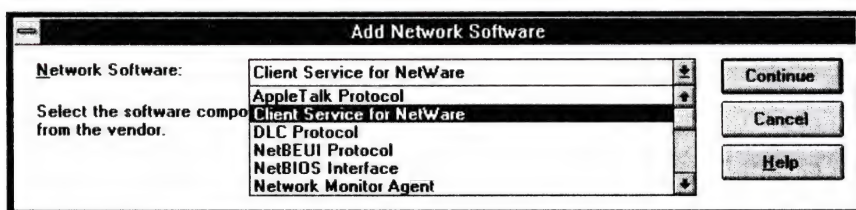
Посмотрим на этот вид доступа с точки зрения обеспечения защиты данных. Допустим, особо важная информация Вашей сети Netware хранится в некоторой базе, управляемой SQL Server, и доступ к базе с клиентских рабочих мест разграничивается средствами SQL Server. Так как файловый доступ с клиентов Netware просто невозможен к серверу NT, то для потенциального взломщика просто не существует “объекта взлома” до тех пор, пока он является обычным клиентом сети Netware. Сам файл базы на сервере достаточно разместить на разделе NTFS и запретить доступ всем, кроме той *учетной записи, от имени которой работает сам SQL Server*. Это служит защитой от физического доступа к файлу из других операционных систем.

Сравните это простое решение с теми ухищрениями, к которым вынуждены прибегать администраторы сети Netware в аналогичных ситуациях, имея старые программы доступа к данным по методу совместного использования файлов (написанных на Clipper, Dbase и т.п.)!

Доступ с Windows NT Server и Windows NT Workstation к серверам Netware

Несмотря на привлекательность описанного выше взаимодействия Windows NT и Netware, продолжали раздаваться требования обеспечить функциональность, позволяющую увидеть сервер Netware с компьютера Windows NT. Сначала планировалось, что эту функциональность обеспечит фирма Novell, но дальше обещаний дело не пошло. И вот незадолго до выхода Windows NT 3.5 появился обеспечивающий нужную функциональность клиент, разработанный Microsoft.

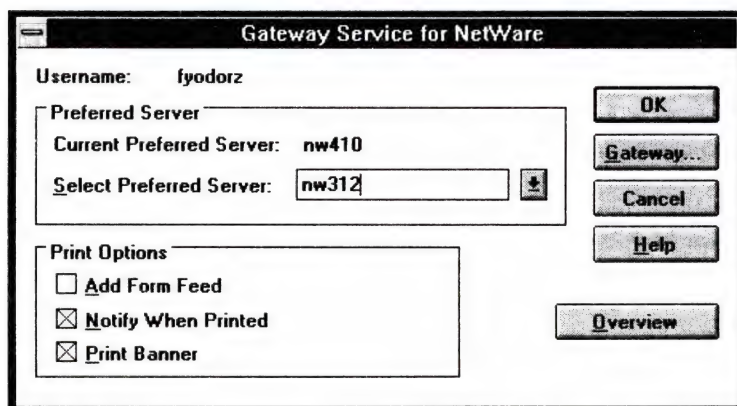
В зависимости от типа системы этот сервис представляется в панели управления под разными именами. В Windows NT Workstation это **Client Service for Netware**, а в Windows NT Server — **Gateway Service for Netware**.



Диалоговое окно установки сервиса доступа к Netware.

Этот сервис позволяет пользователю Windows NT прозрачно осуществлять доступ к файлам и принтерам, предоставляемым в совместное использование на серверах Netware версий 2.x, 3.x и 4.x (в режиме эмуляции Bindery).

После установки этого сервиса каждая регистрация пользователя Windows NT Server сопровождается подключением к предпочтительному (preferred) серверу Netware. Если выбранный сервер в момент входа в систему недоступен, появляется диалоговое окно с предложением выбрать другой.



Диалоговое окно настройки доступа к серверу Netware.

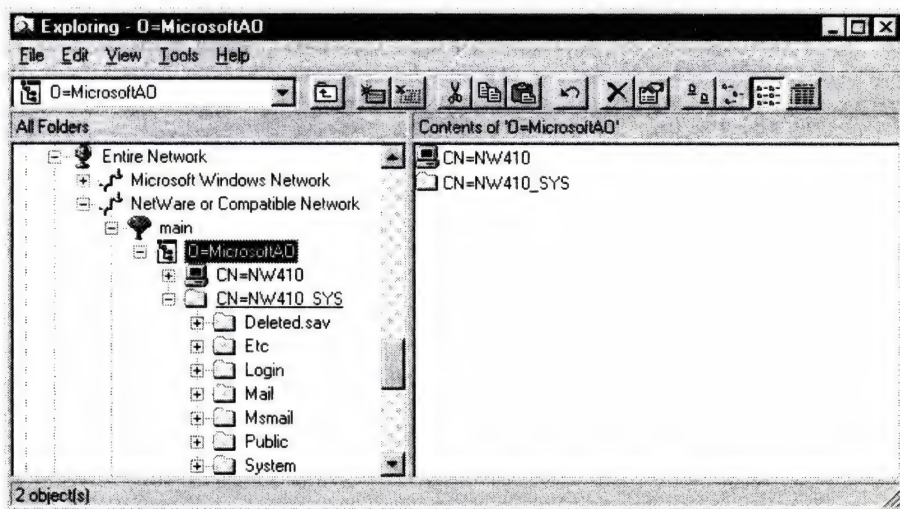
Еще один новый элемент — строка **Netware Compatible Networks** в диалоговом окне **Connect Network Drive** в **File Manager**, под которой перечисляются имена имеющихся в сети серверов Netware. Обладая соответствующими правами, можно подключиться к любому их ресурсу.

Замечание: Осуществляя доступ к серверам Netware, помните, что права и привилегии, которыми Вы обладаете в домене Windows NT, при подключении не имеют никакого значения. Мир Netware продолжает оставаться чужим монастырем и живет по своему уставу — со своими средствами администрирования учетных записей пользователей и средствами разграничения прав доступа. Прежде чем войти в него, убедитесь, что для Вас там создана учетная запись, а Вам сообщен пароль входа.

4.0

Только появился описанный выше сервис, владельцы Netware 4.x заговорили о необходимости реализации поддержки службы каталогов Netware NDS. Такая поддержка была реализована лишь в Windows NT версии 4.0.

Теперь пользователь указывает не предпочтительный сервер, а дерево (tree) — в структуре NDS и необходимый контекст в нем. Если в **Microsoft Explorer** дважды щелкнуть раскидистое дерево, будут показаны его контексты.



При всем при том администрирование сети Netware остается возможным только средствами Netware и невозможно из домена Windows NT.

Обеспечение прозрачного доступа клиентов сети Microsoft к ресурсам сети Novell

Мы уже говорили, что сервис, предоставляющий доступ к серверу Netware со стороны сервера Windows NT, называется **Gateway Service**, т.е. шлюз. И назван он так недаром, поскольку позволяет дополнительно организовать шлюзование из сети Windows в сеть Novell. А вот зачем это нужно, станет ясно из примера.

Предположим, у Вас есть сеть, сервером которой является Windows NT Server, а клиентами — хоть и слабенькие, но еще находящие применение компьютеры с 286 (или 386) процессором и 1Мб оперативной памяти. Они работают по протоколу NetBEUI, и на них установлен стандартный клиент для сети Microsoft Windows. Вместе они работают хорошо, пока не встает задача предоставления клиентам доступа еще и к серверу Netware. Это связано с тем, что нужно добавить а) протокол IPX/SPX и б) соответствующее клиентское программное обеспечение. Наверное, для кого-то 1Мб ОЗУ — очень много, но только не для того, кто устанавливает приложение, работающее в сети, плюс непосредственно сетевой клиент. "Боливар не вынесет двоих" — второй сетевой протокол и клиент просто не влезут в жалкий 1Мб. Тут-то и пригодится шлюзование, позволяющее, не изменяя ничего на клиентах, получить доступ к ресурсам сервера Netware.

Как же организуется шлюз? Для этого создается одна учетная запись, входящая в группу **NTGATEWAY** на сервере Netware, с правами доступа к этому серверу. Все остальные клиенты сервера Windows NT осуществляют доступ к серверу Novell от *имени этой учетной записи*. Неважно, сколько одновременно клиентов воспользуется шлюзом; с точки зрения сервера Netware, это *один пользователь*. Более того, по умолчанию все эти пользователи будут обладать точно такими же правами и привилегиями, какими наделена учетная запись, от имени которой работает шлюз.

Для настройки шлюза в Панели управления предназначена программа конфигурации, позволяющая указать имя учетной записи, от имени которой будет работать шлюз, выбрать сервер Netware и его ресурс, ограничить число пользователей, которые одновременно смогут работать со шлюзом, и ограничить их привилегии. Подключаемый ресурс трактуется системой как ресурс NT Server, предоставляемый в совместное использование. Поэтому-то клиенты, подключенные к серверу, на котором установлен шлюз, могут даже не подозревать о том, что работают с ресурсом Netware сервера, — с их точки зрения, это обычный ресурс Windows NT.

Диалоговое окно New Share для описания параметров шлюза.

При организации шлюза особое внимание обратите на два параметра: привилегии учетной записи, от имени которой работает шлюз, и максимально разрешенное число одновременных подключений. Без особой на то нужды не предоставляйте учетной записи привилегии администратора, так как это значительно повышает риск нарушения защиты Вашей системы.

Создавая шлюз, программа по умолчанию разрешает неограниченное число одновременных подключений. Исходя из лицензионных ограничений, Вы обязаны разрешить лишь столько, сколько лицензий для сервера Netware Вы реально купили, минус 2 (один — подключение самого сервера, второй — подключение шлюза). Поэтому организовать шлюз к серверу, имеющему всего 2 клиентские лицензии, невозможно.



Примечание: Шлюзовый сервис является весьма ресурсоемким. Для его нормального функционирования желательно иметь на сервере не менее 32 Мб оперативной памяти.

Обеспечение прозрачного доступа клиентов сети Netware к файлам и принтерам доменов Windows NT Server

Ну что ж, одна задача решена. Но не кажется ли Вам, что она поставила пользователей сети Microsoft Windows в несколько привилегированное положение? У них прозрачный доступ к двум сетям одновременно, а вот клиенты Netware вынуждены довольствоваться одной своей сетью либо устанавливать дополнительное клиентское обеспечение для доступа к файлам и принтерам NT Server. Хорошо, если таких клиентов у Вас немного, а если несколько десятков? Вспомните и про ограничения, связанные с объемом оперативной памяти.

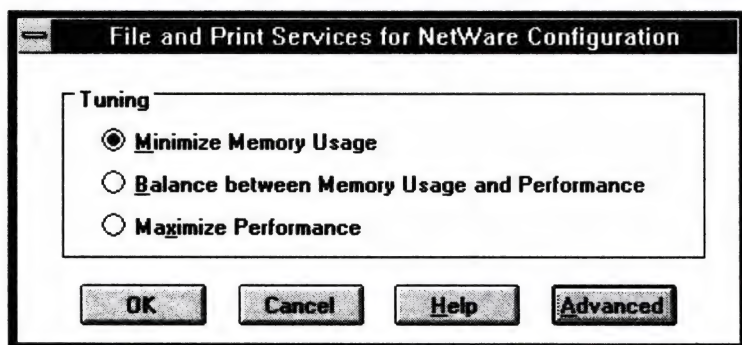
Долгое время многие пользователи мечтали о возможности для NT Server "прикидываться" сервером Netware. Новый программный продукт Microsoft — **File and Print Services for Netware (FPNW)** — сделал мечту реальностью.

Этот сервис устанавливается как еще один дополнительный сетевой сервис. Для его конфигурирования укажите:

- имя сервера, под которым он будет виден для клиентов Netware (по умолчанию это NetBIOS имя компьютера плюс окончание "_FPNW");
- ресурсы, предоставляемые как системный том сервера (SYS:);
- ограничения на доступ к ресурсам.

Уже из перечисленных требований видно, что по сути Вы начинаете администрировать совершенно другой сервер, не имеющий ничего общего с сервером Windows NT.

Установив сервис и перезагрузив компьютер, зайдите в Панель управления, откройте раздел **Network** и, выбрав в списке сетевых сервисов **File and Print Services for Netware**, настройте его производительность.



Диалоговое окно настройки сервиса *File and Print Services for Netware*.

На выбор предлагаются три возможности (см. рисунок):

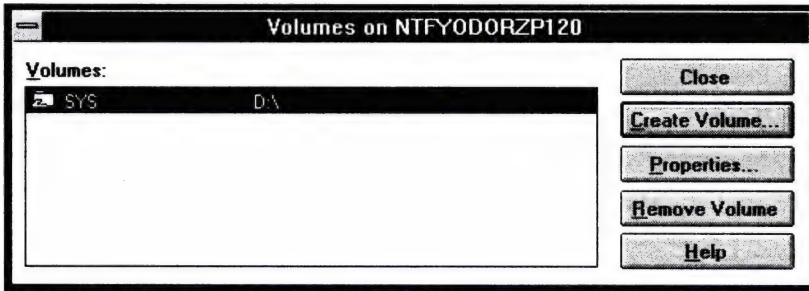
- **Minimize Memory Usage** (минимальное использование памяти);
- **Balance between Memory Usage and Performance** (баланс между использованием памяти и производительностью);
- **Maximize Performance** (максимальная производительность).

То, что Вы укажете, зависит от роли сервера. Если он в основном выполняет функции сервера файлов и печати для сети Windows или является сервером приложений, выберите первую опцию. Если же это только сервер файлов и пе-

части, причем обслуживающий в равной степени пользователей Windows и Netware, выбирается вторая возможность. Ну и наконец, если сервер занимается главным образом обслуживанием клиентов Netware, выбирается третья опция.

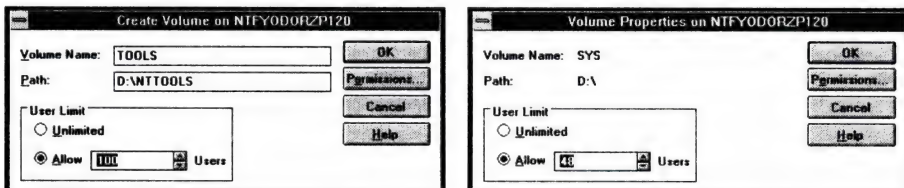
Поскольку на одном и том же компьютере начинают функционировать два совершенно разных сервера, ресурсы, предоставленные через **File Manager** в совместное использование в сети Microsoft Windows, останутся недоступными для клиентов сети Novell. Их надо предоставить повторно, но уже средствами вновь установленного сервиса.

Обратите внимание на новый пункт меню в **File Manager** — **FPNW**: именно здесь содержатся функции предоставления и разграничения доступа. Первое, к чему придется привыкнуть, — это к терминологии, принятой в продуктах Novell. Оперировать придется с томами (volumes), в роли которых Вы можете представить любой каталог на жестких дисках Вашего сервера. Вы можете создавать новые тома, редактировать существующие и удалять ненужные.



Диалоговое окно управления томами сервиса FPNW.

Создавая или редактируя каждый том, можно указать максимальное число одновременных подключений к тому и права доступа к нему. Помните: Вы обязаны указать такое количество одновременных подключений, какое, с одной стороны, не повлияет на производительность сервера, а с другой — не будет противоречить принятой лицензионной политике.



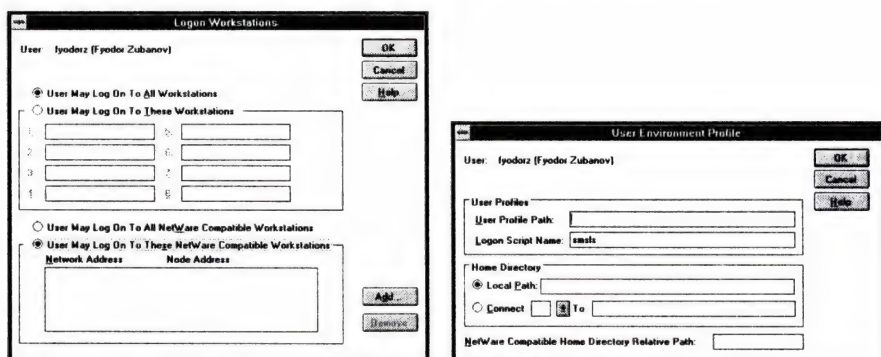
Диалоговые окна *Create Volume* и *Volume properties*.

Определяя права доступа, мы подходим к тому, что объединяет эти два сервера, — к общему механизму защиты Windows NT.

Права доступа можно предоставить лишь для тех учетных записей и групп, что существуют в домене. Клиент сети Netware, не имеющий учетной записи в домене, не сможет воспользоваться этим сервисом точно так же, как в рассмотренном выше примере клиенты сети Windows не могли получить доступ к серверу Netware, не имея на нем учетной записи. Это по-прежнему два разных мира, хоть и обитающие на одной планете.

Кроме того, если созданный том расположен на разделе диска, имеющем формат NTFS, то доступ к файлам и каталогам дополнительно ограничивается списками контроля доступа (см. подробнее главу *Файловая система NTFS*).

Помимо перечисленных, добавляются несколько других параметров, расположенных в диалоговых окнах с соответствующей функциональностью в домене.



Диалоговые окна *Logon Workstations* и *User Environment Profile* после установки FPNW.

В диалоговом окне **Logon Workstations** указываются рабочие станции, с которых возможен вход в домен, принадлежащие не только сети Microsoft Windows, но и Netware.

В диалоговом окне **User Environment profile** можно указать домашний каталог относительно корневого каталога Netware, например D:\SYSVOL.



Внимание: Версия FPNW, выпущенная для Windows NT Server 3.51, несовместима с сервером 4.0. Для него необходимо установить соответствующую версию сервиса.

Централизованное управление серверами Netware

Вспомните, как часто в этой главе мы говорили о “двух мирах”. Содержание различных учетных записей для домена Windows NT и серверов Netware тормозило их совместное использование. Вот почему с таким интересом встречен дополнительный продукт **Microsoft Directory Service Manager for Netware (DSMN)**.

Этот дополнительный сетевой сервис позволяет синхронизировать учетные записи домена NT Server и учетные записи одного или нескольких серверов Netware версий 2.x и 3.x, как бы включив их в один домен. После такой синхронизации пользователи домена Windows NT получают прозрачный доступ к ресурсам серверов Netware и имеют одинаковые права и привилегии, имена учетных записей и пароли.

Для синхронизации сервера с доменом используется утилита **Sincronization Manager**. Выбрав из списка доступных серверов Netware, который необходимо синхронизировать с доменом, Вы можете указать группы пользователей домена, которые будут “делегированы” на выбранный сервер.



Внимание: Для подключения к выбранному серверу используется учетная запись с правами супервизора (**Supervisor**) на выбранном сервере.

Указать список групп можно вручную или создав файл (mapping file), в котором перечислены необходимые группы. Удобно создать специальную группу в домене (например, Novell Users), включив в нее учетные записи пользователей, которые должны иметь доступ к определенному серверу Netware.

Важная особенность этой утилиты — возможность выполнения пробной синхронизации (**Trial Synchronisation**). Более того, настоятельно рекомендуется выполнять эту процедуру при каждом подключении к домену нового сервера.

Directory Service Manager for NetWare автоматически синхронизирует включенные в домен и временно не работавшие серверы. После подключения к сети такой сервер можно синхронизировать принудительно, не дожидаясь выполнения обычного цикла синхронизации. Для этого используется одна из следующих команд:

Synchronize Selected Server — посылает обновленную информацию об учетных записях на выбранный сервер NetWare. Посылается информация только об учетных записях, еще не полученных этим сервером.

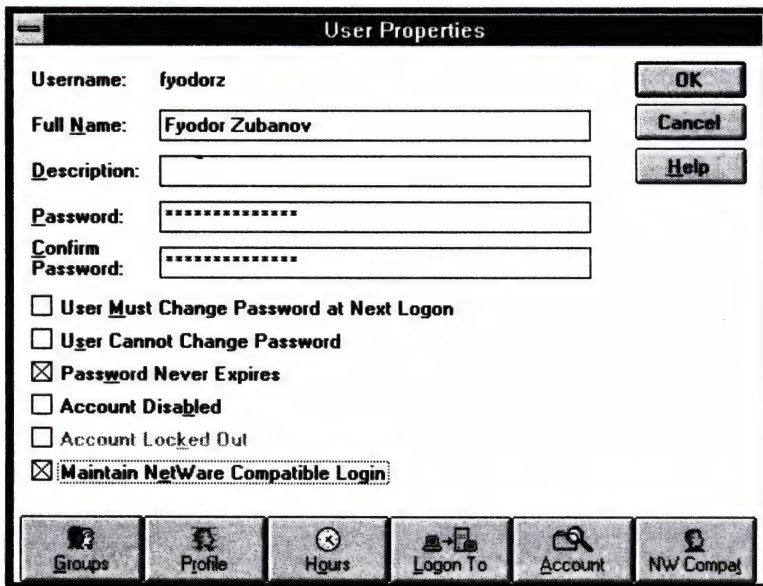
Synchronize All Servers — посылает информацию об обновленных учетных записях на все серверы NetWare в домене. Каждый сервер получает только необходимую информацию об обновлениях.

Fully Synchronize Selected Server — посылает всю информацию об учетных записях на выбранный сервер NetWare. Эта команда используется только при полной рассинхронизации сервера с доменом.

Fully Synchronize All Servers — посылает всю информацию об учетных записях на все серверы NetWare, включенные в домен. Эта команда используется только при полной рассинхронизации нескольких серверов.

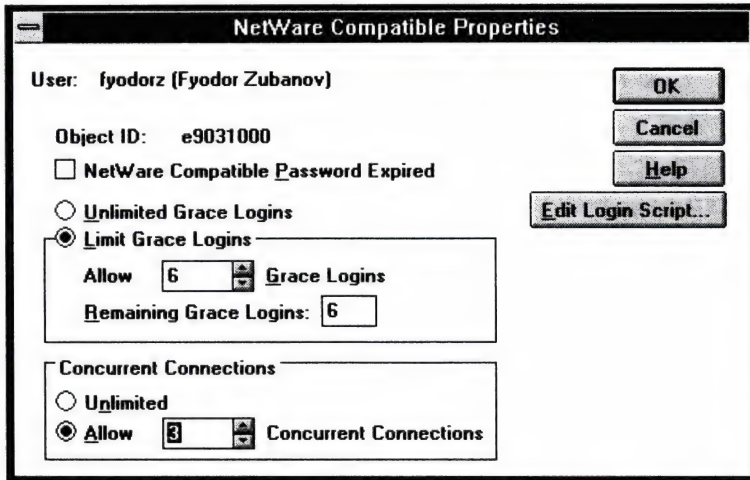
После установки **DSMN** внешний вид диалогового окна **User Properties** (в **User Manager for Domains**) несколько меняется за счет добавления нового флажка **Maintain Netware Compatible Logins** и кнопки **NW Compat**.

Эти новые функции становятся доступными только для учетных записей, делегированных хотя бы на один сервер Netware. Но реально член группы, делегированной на сервер, получит доступ к его ресурсам только после того, как для него будет отмечен флажок **Maintain Netware Compatible Logins**.



Диалоговое окно **User Properties** после установки **DSMN**.

В диалоговом окне *NetWare Compatible Properties* указываются параметры, значительно влияющие на защищенность Вашей системы и во многом аналогичные тем, что задаются в диалоговом окне *Account Policy* (см. раздел *Управление политикой ведения учетных записей*).



Диалоговое окно *Netware Compatible Properties*.

Подчеркну: несмотря на то, что сервер как бы включается в домен, политика ведения учетных записей остается у него самостоятельной, хоть и управляется средствами NT Server.

А вот параметры, влияющие на защищенность системы:

Netware Compatible password Expired — отметьте этот флажок для ограничения срока жизни пароля. И тогда при первой же регистрации в домене пользователю Netware будет предложено изменить пароль. Отмечая этот флажок, предоставьте хотя бы одно значение ***Grace Login***.

Limit Grace Logins — число дополнительных попыток регистрации в системе после истечения срока жизни пароля. Эти попытки предоставляют пользователю возможность изменить пароль.

Concurrent Connections — число одновременных подключений к серверу. Для единообразия с серверами Windows NT установите неограниченное число подключений (***Unlimited***).

Login Script — чтобы отредактировать сценарий регистрации на сервере Netware, щелкните кнопку ***Edit Login Script***.



Внимание: Версия **DSMN**, выпущенная для Windows NT Server 3.51, несовместима с сервером версии 4.0. Для него необходимо установить соответствующую версию сервиса.

Переход от сервера Netware к Windows NT Server

Полностью перейти с Netware на Windows NT администраторы сети могут заставить разные причины. Как выполнить такой переход быстро и безопасно, не потеряв ни данных, ни пользователей? Можно, конечно, вручную создать учетные записи для всех пользователей сервера Netware в домене Windows NT, прописать им соответствующие права и привилегии, исправить сценарии входа в систему, перенести принадлежащие им ресурсы и т.д. Представляете, сколько это займет времени и сколько ошибок при этом можно допустить, если у Вас несколько серверов и сотни пользователей?

Для облегчения такой задачи в Windows NT Server имеется утилита **Migration Tool for Netware**. По умолчанию для нее не создается значок в **Program Manager**, поэтому многие даже и не подозревают о ее существовании. Для работы с этим инструментом запустите файл %systemroot%\system32\nwconv.exe.

Migration Tool позволяет перенести учетные записи пользователей и групп, а также файлы и каталоги с серверов NetWare 2.x и 3.x на компьютеры с Windows NT Server, полностью сохранив информацию об учетных записях и атрибуты защиты файлов и каталогов.

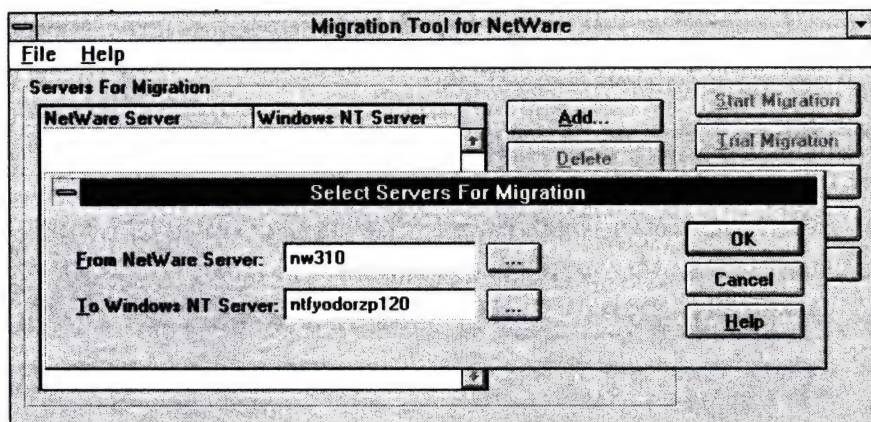


Замечание: Информация о защите файлов и каталогов сохранится только при переносе их на раздел NTFS.



Внимание: Для осуществления переноса необходимо минимум 2 компьютера: сервер Netware и сервер Windows NT. Перед выполнением переноса установите на NT Server сервисы **NWLink IPX/SPX compatible** и **Gateway service for Netware**. Кроме того, зарегистрируйтесь на сервере Netware с правами супервизора (**Supervisor**), а на сервере NT надо быть членом группы администраторов.

Запустив утилиту, в появившемся диалоговом окне укажите сервер Netware, с которого выполняется перенос, и сервер Windows NT, на который переносятся данные. Можно указать несколько серверов того и другого типа.



Окно программы *Migration Tool for Netware*.

Важная особенность этой программы — возможность выполнить пробную миграцию (***Trial migration***), что позволит исключить ошибки переноса.

Перенос учетные записи групп и пользователей с сервера NetWare на компьютер с Windows NT Server, ***Migration Tool*** автоматически создает учетные записи на первичном контроллере того домена, в который входит выбранный сервер. Потом они тиражируются на другие контроллеры домена.

По умолчанию переносятся учетные записи всех пользователей сервера NetWare, кроме тех, чьи имена совпадают с уже существующими в домене. При этом в журнал заносится сообщение об ошибке, которое можно проанализировать во время выполнения пробного переноса. Если имя переносимой группы совпадает с именем группы в домене, эта группа также не будет перенесена, но сообщение об ошибке в журнал не заносится.

Дополнительно используются следующие умолчания переноса:

- переносимые учетные записи теряют пароль;
- переносятся ограничения, накладываемые на пароли на сервере NetWare, и параметры блокировки учетных записей;
- группы и пользователи с правами ***Supervisor***, ***Workgroup Manager*** и ***User Account Manager*** переносятся в домен Windows NT без административных привилегий.

Выполнив пробную миграцию и анализ журнала (файл LOGFILE.LOG), можно подстроить параметры переноса или использовать файл соответствий для корректировки следующих параметров:

- перенос только файлов и каталогов;
- пароль, равный имени пользователя или одинаковый для всех;
- способ обработки совпадающих имен пользователей;
- способ обработки совпадающих имен групп;
- ограничения учетных записей, принятые в Windows NT по умолчанию;
- добавление пользователей с правами Supervisor в административную группу Windows NT.

При переносе файлов и каталогов с сервера NetWare на сервер Windows NT права доступа к ним транслируются в соответствующие права Windows NT.

Ниже приведена схема трансляции прав доступа к каталогам.

<i>NetWare</i>	<i>Windows NT</i>
Supervisory (S)	Full Control (All) (All)
Read (R)	Read (RX) (RX)
Write (W)	Change (RWXD) (RWXD)
Create (C)	Add (WX) (not specified)
Erase (E)	Change (RWXD) (RWXD)
Modify (M)	Change (RWXD) (RWXD)
File Scan (F)	List (RX) (not specified)
Access Control (A)	Change Permissions (P)

В следующей таблице показано соответствие прав доступа к файлам:

<i>NetWare</i>	<i>Windows NT</i>
Supervisory (S)	Full Control (All)
Read (R)	Read (RX)
Write (W)	Change (RWXD)
Erase (E)	Change (RWXD)
Modify (M)	Change (RWXD)
Access Control (A)	Change Permissions (P)

Права **Create** (C) и **File Scan** (F) игнорируются при переносе файлов.

Кроме прав доступа, выполняется перенос атрибутов файлов. В следующей таблице приведено соответствие между атрибутами:

Атрибуты файлов NetWare**Атрибуты файлов Windows NT**

Read Only (Ro)	Read Only (R)
Delete Inhibit (D)	Read Only (R)
Rename Inhibit (R)	Read Only (R)
Archive Needed (A)	Archive (A)
System (SY)	System (S)
Hidden (H)	Hidden (H)
Read Write (Rw)	Нет – файлы, не имеющие атрибута R, доступны и для чтения, и для записи.

Следующие атрибуты файлов NetWare не поддерживаются в Windows NT и игнорируются: **Copy Inhibit** (C), **Execute Only** (X), **Indexed** (I), **Purge** (P), **Read Audit** (Ra), **Shareable** (SH), **Transactional** (T), и **Write Audit** (Wa).

Так же, как и в Windows NT Server, учетные записи пользователей Netware могут иметь различные ограничения. В приведенных ниже таблицах показано соответствие переносимых ограничений в двух случаях: при переносе на компьютер с установленным сервисом **File and Print Services for Netware** и на компьютер, на котором он не установлен.

Перенос ограничений учетных записей Netware на сервер Windows NT без установленного сервиса FPNW

Ограничения учетных записей Netware	Эквивалент Windows NT Server	Как выполняется перенос
Expiration Date	Expiration Date	Для каждой индивидуальной учетной записи.
Account Disabled	Account Disabled	Для каждой индивидуальной учетной записи.
Limit Concurrent Connections	Отсутствует	Не переносится.
Require Password	Permit Blank Password	В виде политики всех учетных записей.
Minimum Password Length	Minimum Password Length	В виде политики всех учетных записей.
Force Periodic Password Changes	Password Never Expires	Для каждой индивидуальной учетной записи.
Days between forced changes	Maximum Password Age	В виде политики всех учетных записей.
Grace Logins	Отсутствует	Не переносится.
Allow user to change password	User cannot change password	Для каждой индивидуальной учетной записи.

Перенос ограничений учетных записей Netware на сервер Windows NT без установленного сервиса FPNW (продолжение)

Ограничения учетных записей Netware	Эквивалент Windows NT Server	Как выполняется перенос
Require unique passwords	Password uniqueness	В виде политики всех учетных записей.
Station restrictions	Отсутствует	Не переносится.
Time Restrictions	Logon Hours	Для каждой индивидуальной учетной записи.
Intruder Detection/Locout	Account Locout	В виде политики всех учетных записей.
User disk volume restrictions	Отсутствует	Не переносится.

Дополнительные ограничения учетных записей, переносимые на компьютер с установленным сервисом FPNW

Ограничения бюджетов Netware	Эквивалент Windows NT Server (с FPNW)	Как выполняется перенос
Limit Concurrent connections	Limit Concurrent connections	Для каждой индивидуальной учетной записи.
Grace Logins	Grace Logins	Для каждой индивидуальной учетной записи.
Station restrictions	Station restrictions	Не переносится.
Login Scripts	Login Scripts	Для каждой индивидуальной учетной записи.

Завершив процедуру переноса, замените клиентское программное обеспечение на бывших рабочих станциях сети Netware — это позволит им сразу зарегистрироваться в домене Windows NT. Если Вы указали на необходимость незамедлительной смены пароля для вновь добавленных пользователей, они это сделают при первой регистрации, снизив тем самым вероятность проникновения посторонних в сеть.

Построение глобальных сетей и работа с Internet

Глобальная сеть требует обеспечения связи между несколькими локальными, так чтобы пользователи не задумывались о получении и безопасности доступа к ресурсам в удаленной сети. Заманчивая перспектива задействовать для этих целей Internet до недавнего времени отвергалась из-за очень высокой степени риска проникновения в корпоративную систему не в меру любопытного "хакера". Разработанные для Windows NT новые средства позволяют отнестись к этой проблеме с большим оптимизмом.

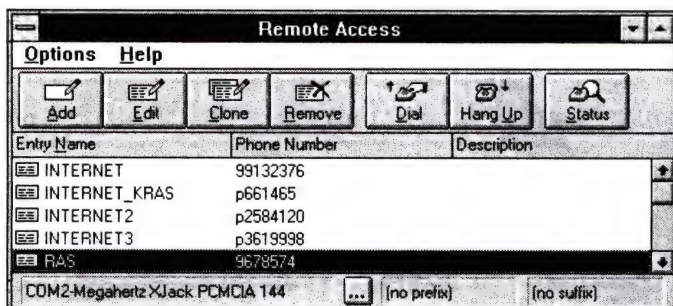


Удаленный доступ в Windows NT

При словах "глобальная сеть" Вы, конечно, сразу вспомните об Internet — первой общедоступной глобальной сети. Возникнут мысли о процессе подключения к Internet, телефонных линиях, маршрутизации, адресных сетках и т.п. Вместе с тем в глобальную корпоративную сеть объединяют сети большого предприятия. Такие сети есть, например, в компаниях Microsoft, Digital, IBM и др. Кроме того, в любой организации хватает мобильных пользователей, путешествующих по всему свету с ноутбуками. Возможность подключения к корпоративной сети в любой точке земного шара им нужна, как воздух.

В сетях, построенных на основе Microsoft Windows NT, средством объединения локальных сетей является Сервер удаленного доступа (Remote Access Server — RAS), позволяющий удаленным пользователям работать так, будто они подключены непосредственно к сети. Соединение по RAS прозрачно и для клиентов, и для сетевых приложений.

Клиентами сервера удаленного доступа могут быть пользователи Windows NT, Windows 95, Windows for Workgroups, MS-DOS (с установленным сетевым клиентом Microsoft), клиенты RAS LAN Manager и любой PPP-клиент.



Диалоговое окно Remote Access.

Windows NT Server RAS позволяет одновременно подключаться 256 удаленным клиентам. К Windows NT Workstation может подключиться только один удаленный клиент. RAS поддерживает протоколы:

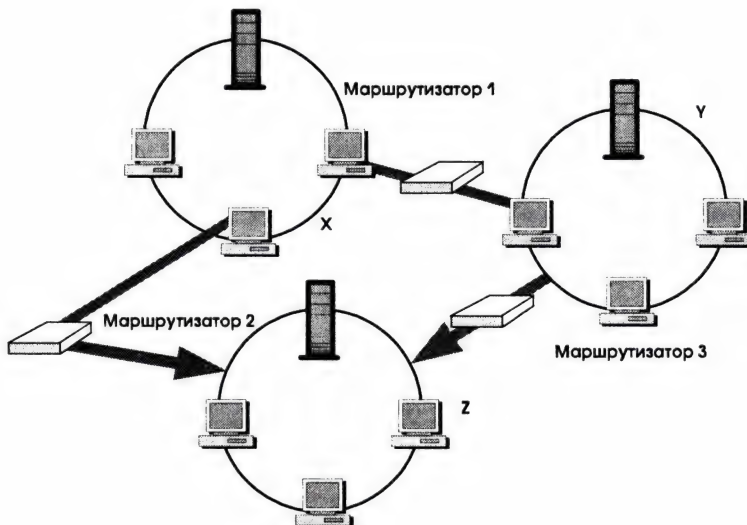
- IP для доступа к сетям TCP/IP, таким как Internet;
- IPX для доступа к серверам и принтерам NetWare;
- NetBIOS поверх IPX, TCP/IP или NetBEUI;
- встроена поддержка приложений, использующих Windows Sockets поверх TCP/IP или IPX, named pipes, Remote Procedure Call (RPC) и LANManager API.

Подключение к RAS-серверу производится через обычные телефонные или выделенные линии с одним модемом или пулом модемов. Более быстрая связь обеспечивается сетями ISDN или X.25. В Windows NT 4.0 поддерживается подключение через порт RS-232C (нуль-модем) или с протоколом Point To Point Tunelling Protocol (PPTP).

RAS позволяет использовать также сервер Windows NT в качестве хоста Internet и предоставлять доступ по PPP. Развитые функции защиты делают безопасным подключение через сервер удаленного доступа.

Маршрутизация в Windows NT

Глобальную сеть невозможно построить без *маршрутизации*. *Маршрутизаторы* позволяют осуществлять взаимодействие между локальными и глобальными сетями и сетями с различной топологией (например, Ethernet и Token Ring). В каждом пакете, пересылаемом в локальной сети, имеется *заголовок*, поля которого содержат адреса исходный и назначения. Сравнив заголовки пакетов с сегментами сети, маршрутизаторы выбирают наилучший путь для их прохождения, что повышает производительность сети. На рисунке для пакета, передаваемого с компьютера X на компьютер Z, лучший путь — через наименьшее число маршрутизаторов. Даже если маршрутизатор 1 установлен для компьютера X по умолчанию, пакет все равно будет послан через маршрутизатор 2, а компьютер X будет уведомлен о наилучшем маршруте к компьютеру Z.



Маршрутизация в сети.

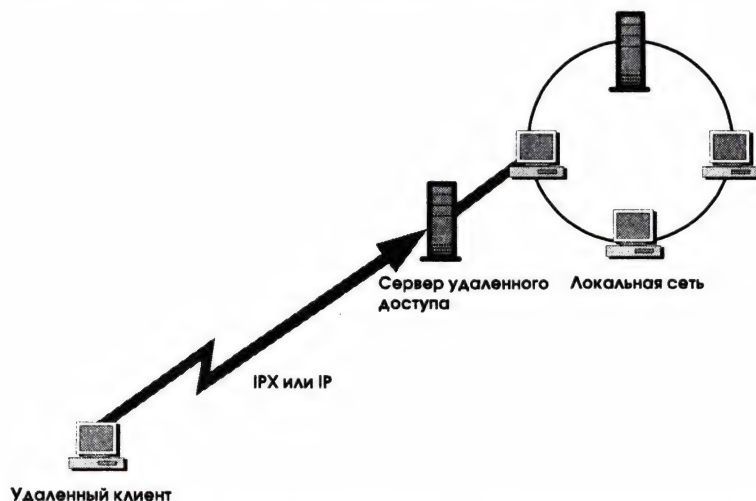
Многопротокольная маршрутизация в Windows NT Server

Возможности многопротокольной маршрутизации (**Multiprotocol Routing — MPR**) появились в Windows NT Server 3.51 с выходом пакета исправлений 2 (Service Pack 2), т.е. как дополнительный продукт. В четвертой версии эта возможность встроена в систему.

MPR, содержащий функции маршрутизации RIP (Routing Information Protocol), позволяет использовать Windows NT Server как маршрутизатор между двумя или несколькими сетями с применением RIP на IP, IPX или на том и другом одновременно. Компьютер может выступать и в качестве агента передачи DHCP (DHCP Relay agent), что делает возможной передачу сообщения DHCP по сети IP.

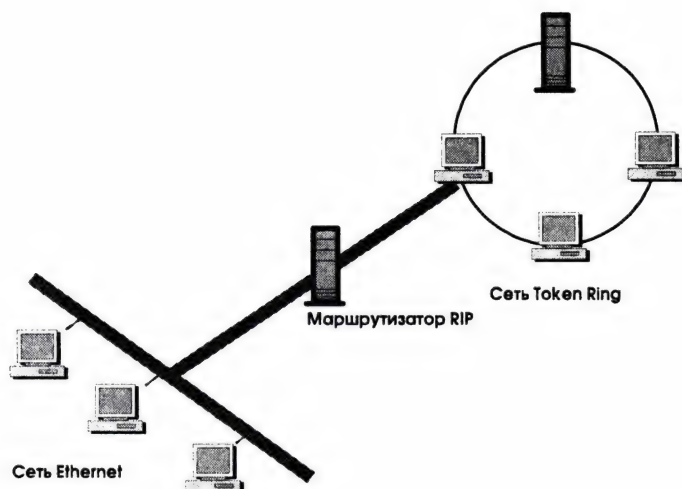
Возможности маршрутизации

В Windows NT Server сервер удаленного доступа (Remote Access Server — RAS) можно использовать для организации маршрутизации между удаленным клиентом и локальной сетью, как показано на рисунке:



Маршрутизация между удаленным клиентом и локальной сетью.

Можно организовать маршрутизацию между двумя локальными сетями:



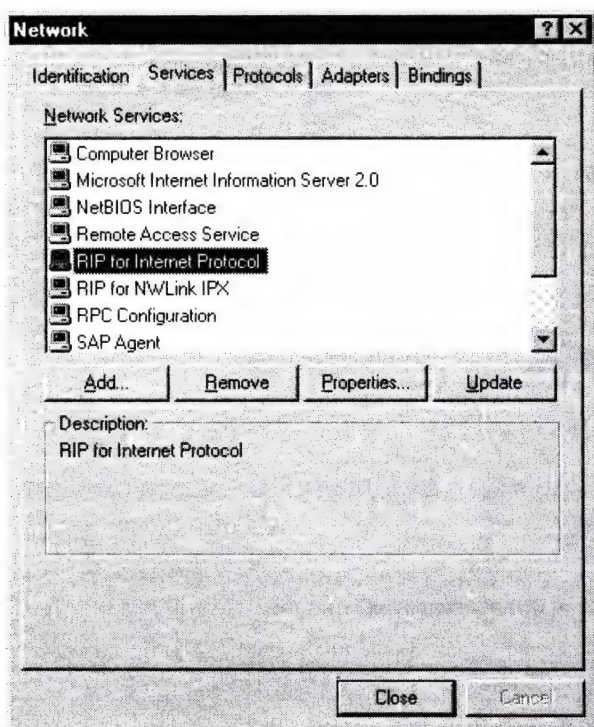
Маршрутизация между двумя локальными сетями.

Организовать маршрутизацию между глобальными сетями через коммутируемые или обычные телефонные линии невозможно. Единственное исключение — плата доступа к глобальной сети (WAN card), например, T1 или Frame Relay, которая с точки зрения маршрутизатора выглядит как сетевая плата.

Установка маршрутизации между локальными сетями

На компьютере с Windows NT Server, исполняющем роль маршрутизатора, должны быть минимум две сетевые платы. В зависимости от сети можно установить поддержку маршрутизации по IP или по IPX. Перед установкой убедитесь, что нужные протоколы в системе уже активны.

Для установки межсетевой маршрутизации откройте **Control Panel**, вызовите раздел Network, щелкните вкладку **Services** и добавьте **RIP for Internet Protocol** или **RIP for NWLink IPX/SPX Compatible Transport**. Во время установки RIP для NWLink IPX появится сообщение о том, что передача NetBIOS Broadcast (тип 20) неактивна. Если Вы используете NetBIOS поверх IPX, разрешите распространение пакетов типа 20.



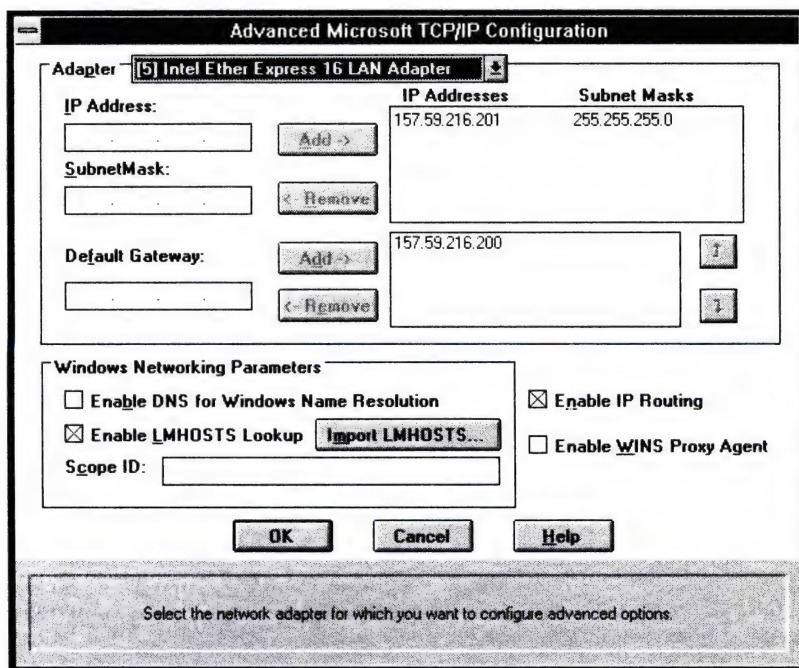
Диалоговое окно *Network Services*. Установив маршрутизацию RIP на IPX, сконфигурируйте протокол IPX для разрешения маршрутизации: выбрав в **Control Panel** настройки протокола IPX, отметьте флажок **Enable RIP Routing**.

RIP для IP устанавливается как сервис и активизируется автоматически. Как и любой сервис, его можно запускать или останавливать в любой момент в соответствующем разделе в **Control Panel**.

Статическая маршрутизация по IP

Для IP существует два типа маршрутизации: статическая и динамическая. При первой Вы ограничены фиксированными *таблицами маршрутов* (routing table). При второй таблицы маршрутов автоматически обновляются: это снимает часть забот с администратора, но увеличивает трафик в больших сетях.

Чтобы задать статическую маршрутизацию, удалите сервис **RIP for IP** (если Вы его уже поставили), а в **Control Panel** выберите установки протокола TCP/IP и, щелкнув кнопку **Advanced**, отметьте флажок **Enable IP Routing**. Эта опция неактивна, если в компьютере установлена только одна сетевая плата.



Установка статической маршрутизации.

4.0

В Windows NT 4.0 в окне настроек протокола TCP/IP щелкните вкладку **Routing** и отметьте флажок **Enable IP Forwarding**.

Далее может потребоваться корректировка таблицы маршрутов командой **route**, работа с которой подробно описана в документации на Windows NT Server.

Маршрутизация через коммутируемый канал связи

Сервер удаленного доступа в Windows NT Server не предназначен для маршрутизации пакетов между локальными сетями через коммутируемые каналы связи. Однако при правильной конфигурации компьютеров, выполняющих роль RAS-серверов, и других компьютеров в небольшой локальной сети RAS-сервер можно использовать как маршрутизатор к Internet или большой сети предприятия по TCP/IP.

Чтобы организовать маршрутизацию между локальной сетью и Internet через коммутируемую линию, требуются:

- компьютер с установленной Windows NT и подключенными сетевой платой и высокоскоростным модемом (или линией ISDN);
- подключение к Internet или сети предприятия по протоколу PPP (Point to Point Protocol);
- сеть или подсеть, отличная от подсети поставщика услуг Internet (Internet Service Provider — ISP);
- правильно определенные в реестре параметры конфигурации компьютера, выступающего в роли маршрутизатора, а также компьютеров-клиентов (параметры описаны ниже);
- небольшая по размеру сеть, не требующая динамической маршрутизации, обеспечиваемой RIP (справедливо для сетей, рост которых не предвидится в будущем).

Чтобы использовать имена, а не только IP-адреса, получите имя домена с помощью ISP.

Итак, получив PPP-подключение, IP-адреса для своей подсети (и правильную маску подсети) и (дополнительно) имя домена, можно сконфигурировать RAS и остальные компьютеры для работы со шлюзом в Internet.

Параметры организации маршрутизации

1. На RAS-компьютере, выступающем в качестве маршрутизатора в Internet, добавьте в реестре новое значение:

Ветвь	HKEY_LOCAL_MACHINE
Ключ	System\CurrentControlSet\Services\RasArp\Parameters
Параметр	DisableOtherSrcPackets
Тип	REG_DWORD
Значение	0

По умолчанию в заголовок каждого пакета, передаваемого с RAS-компьютера по PPP-линии, вставляется адрес этого компьютера в качестве адреса-источника. Так как у пакетов, приходящих на сервер удаленного доступа с других компьютеров, другие адреса источников, установите параметр ***DisableOtherSrcPackets*** равным 0, чтобы они просто передавались через PPP.

2. Если Ваша подсеть принадлежит к той же логической подсети, что и сеть ISP, установите новое значение в реестре компьютера, выполняющего роль маршрутизатора.

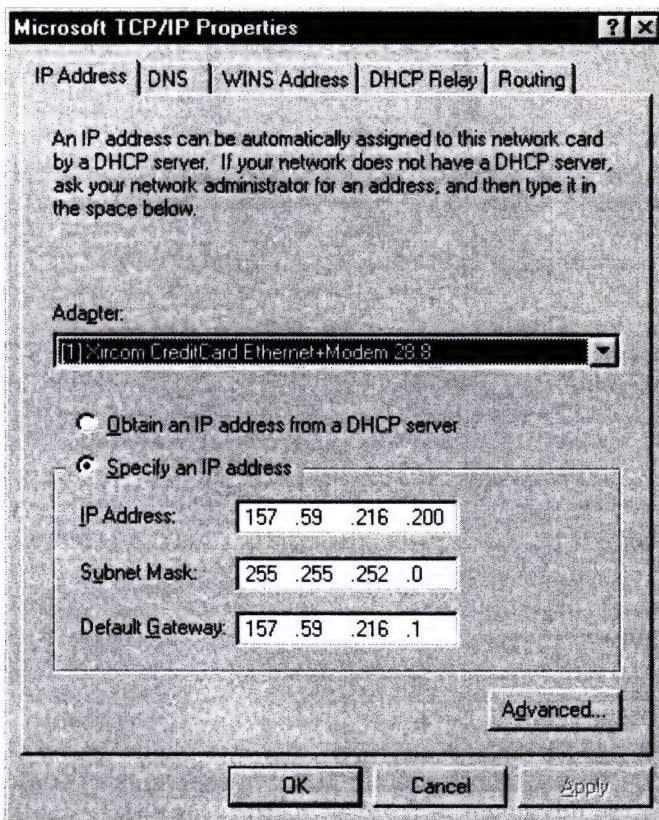
Ветвь	HKEY_LOCAL_MACHINE
Ключ	System\CurrentControlSet\Services\RasMan\PPP\IPCP
Параметр	PriorityBasedOnSubNetwork
Тип	REG_DWORD
Значение	1

Компьютер можно подключить к локальной сети через сетевую плату и RAS. Если RAS и сетевая плата принадлежат одной сети, а также отмечен флажок **Use Default Gateway On Remote Network**, все пакеты посылаются через RAS, хотя два адреса располагаются в разных подсетях одной сети.

Например, если сетевой плате назначен адрес 17.1.1.1 (маска 255.255.0.0), а для RAS — 17.2.1.1, то через RAS будут посылаться все пакеты 17.x.x.x. Если установить указанный выше параметр, то пакеты 17.2.x.x будут пересылаться через RAS, а пакеты 17.1.x.x — через сетевую плату.

3. Сконфигурируйте шлюз, выбираемый по умолчанию (default gateway) на всех компьютерах локальной сети.

Шлюз устанавливается в параметрах протокола TCP/IP в **Control Panel**.



На всех компьютерах Вашей локальной сети в качестве **Default Gateway** укажите адрес сетевой платы компьютера, выполняющего роль маршрутизатора, а на нем самом этот параметр оставьте незаполненным. На рисунке показан пример конфигурации сети:

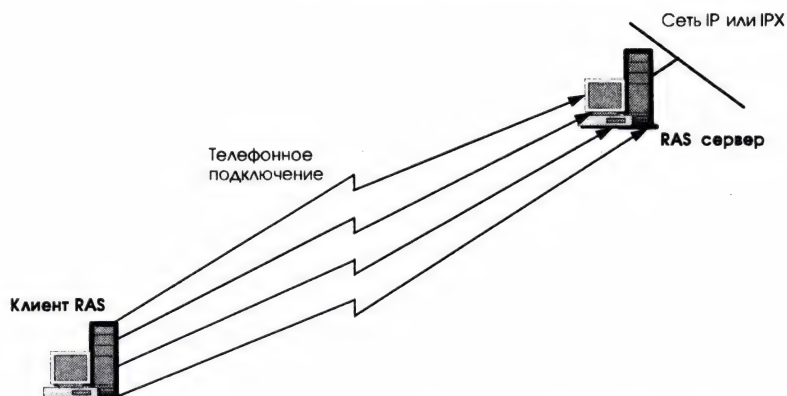


Пример конфигурации для маршрутизации между локальной сетью и Internet.

Повышение пропускной способности канала

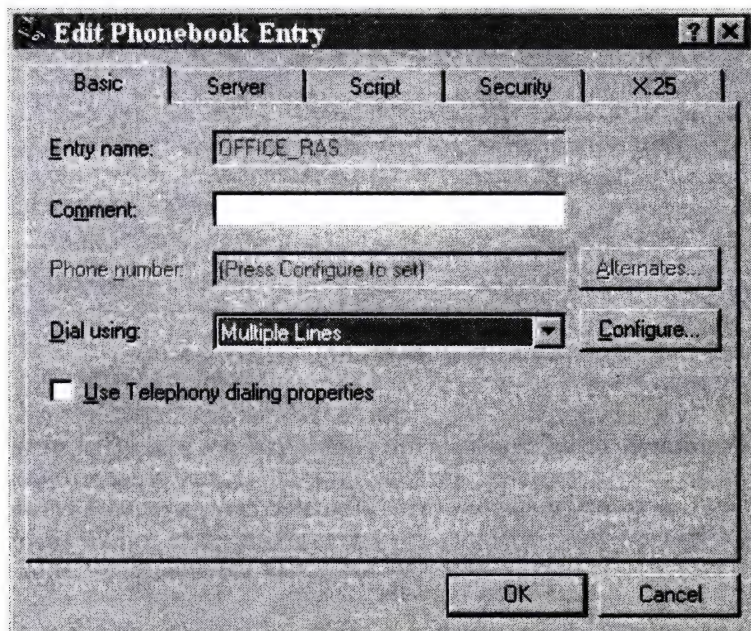
Используя в качестве линии связи между двумя локальными сетями телефонные каналы, Вы обрекаете себя на довольно низкую скорость обмена. Сегодня это 9600-19200 Кбит/сек. Конечно, для нормального взаимодействия двух локальных сетей этого явно недостаточно.

Multilink — новая возможность Windows NT 4.0 — позволяет соединить два компьютера по нескольким телефонным каналам параллельно. Суммарная пропускная способность такого канала увеличивается пропорционально числу задействованных телефонных линий.



Использование параллельных телефонных каналов для повышения пропускной способности.

Для обеспечения этой возможности в параметрах сервиса удаленного доступа на сервере отметьте флажок **Enable Multilink**. На клиентской стороне в настройках конкретного соединения вместо конкретного порта и модема укажите **Multiple Lines**. Данная функция доступна как для модемной связи, так и для сетей ISDN. При инициации связи со стороны клиента будет одновременно осуществляться доступ по всем каналам сразу.



Настройка клиента на использование сразу нескольких каналов связи.

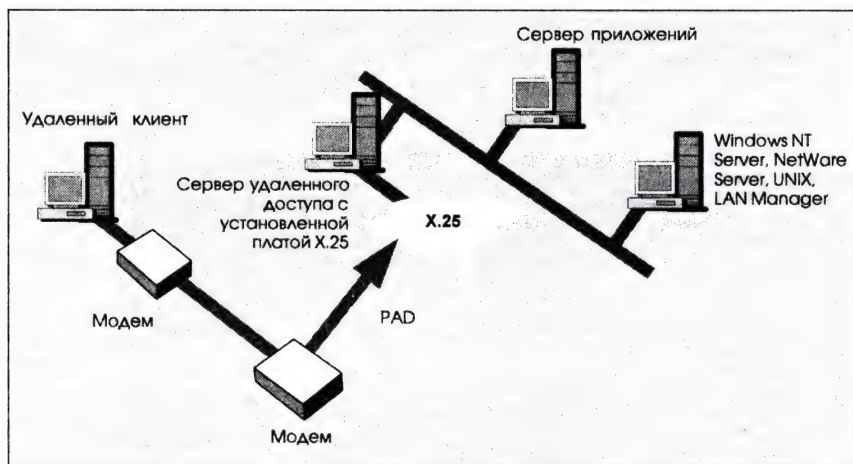
Сети X.25

Windows NT RAS поддерживает подключение к сетям X.25. Доступ можно осуществить двумя способами: через Асинхронные ассемблеры/дизассемблеры пакетов (Asynchronous Packet Assembler/Disassembler — PAD) и непосредственно — через специальные платы (smart cards). Первое используется только для клиентов (Windows или Windows NT), а второе — как для клиентов, так и для серверов.



Внимание: Текущая версия сервера удаленного доступа поддерживает работу только с PAD, настроенными на передачу 8 битов данных, 1 стоп-бита и отсутствие бита четности. Обратитесь к документации на используемый PAD, чтобы сконфигурировать его соответствующим образом.

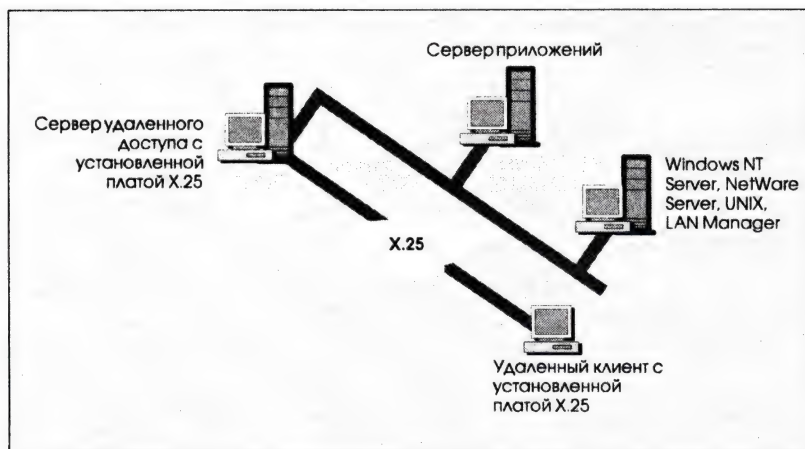
На рисунке показано подключение клиента к сети корпорации через сеть X.25 с использованием PAD. Получив пакет из сети X.25, PAD преобразует его в пакет коммуникационной линии, а пакеты, поступающие из нее — в пакеты X.25. Это делает возможным взаимодействие между клиентом и удаленной сетью.



Подключение клиента к корпоративной сети через сеть X.25 с использованием PAD.

Кроме подключения через PAD, две сети можно связать и непосредственно по X.25. Для этого в компьютерах, функционирующих как серверы удаленного доступа, установите специальные платы, выполняющие роль PAD. С точки зрения сервера, они являются набором портов связи (иногда — обычной сетевой

платой). На рисунке показано непосредственное подключение клиента к сети через X.25.



Непосредственное подключение клиента к корпоративной сети через сеть X.25.

В таблице сравнивается непосредственный тип подключения с подключением через PAD.

PAD

Экономия за счет отказа от использования выделенных линий.

Позволяет подключаться из любого места, где есть телефон: отеля, аэропорта, квартиры и т.д.

Требуется два шага для подключения.

Ограничивает скорость связи максимальной скоростью линий и используемых модемов.

Меньше возможностей по настройке PAD.

Доступен только для клиентской части.

Непосредственное подключение

Требует дорогих выделенных линий.

Подключение возможно только из определенных мест.

Соединение устанавливается за один шаг.

Используется скорость выделенной линии (56 К).

Более высокая надежность.

Доступно как клиенту, так и серверу.

Для обеспечения работы установите у специализированной платы X.25 следующие X.3-параметры.

Номер параметра	Параметр X.3	Величина
1	PAD Recall	0
2	Echo	0
3	Data Fwd. Char	0
4	Idle Timer	1
5	Device Ctrl	0
6	PAD Service Signals	1
7	Break Signal	0
8	Discard Output	0
9	Padding after CR	0
10	Line Folding	0
11	не устанавливается	
12	Flow Control	0
13	Linefeed Insertion	0
14	Padding after LF	0
15	Editing	0
16	Character Delete	0
17	Line Delete	0
18	Line Display	0
19	Editing PAD Srv Signal	0
20	Echo mask	0
21	Parity Treatment	0
22	Page Wait	0

Для организации маршрутизации между локальными сетями, соединенными X.25, устанавливается дополнительный продукт фирмы EICON Technologies — **WAN Services for Windows NT** и описанный выше **Multiprotocol Router (MPR)**. С точки зрения этого пакета, специализированная плата X.25 является обычной сетевой платой, что позволяет организовать маршрутизацию RIP.

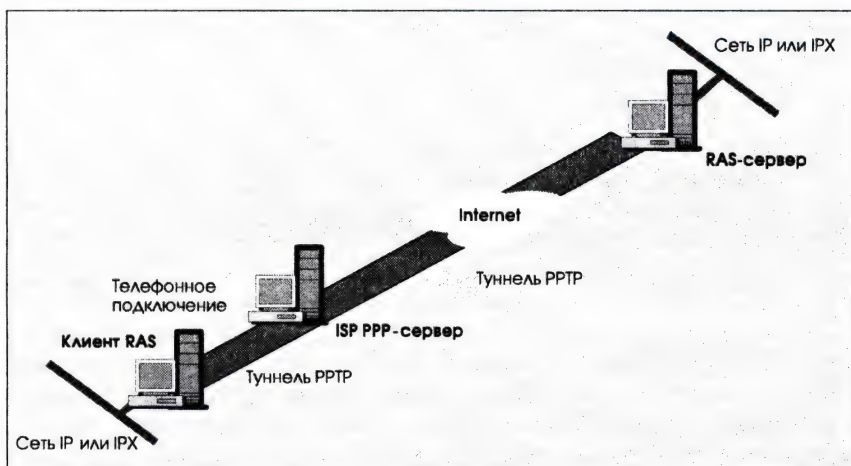
Point-to-Point Tunelling Protocol (PPTP)



- Новая сетевая технология PPTP, появившаяся в 4 версии Windows NT, позволяет организовать виртуальные корпоративные сети (ВКС) путем безопасного соединения локальных сетей через Internet.
- PPTP делает возможным перенос всей аппаратной части (модемов или плат ISDN) с сервера удаленного доступа Windows NT на Фронтальные

Процессоры (Front-End Processors — FEP). Благодаря PPTP клиенты могут осуществлять доступ к корпоративной сети из любой точки земного шара, подключившись к Internet (через ISP или непосредственно). В любом случае такое подключение выполняется совершенно безопасно и использует механизмы шифрования. Поддерживаются протоколы IP, IPX и NetBEUI.

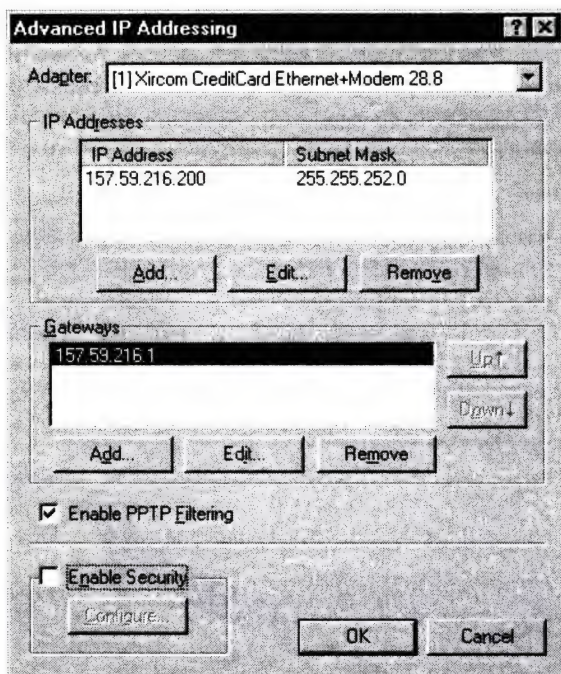
PPTP рассматривает существующую корпоративную сеть как PSTN, ISDN или X.25-сеть. Виртуальная глобальная сеть поддерживается общедоступными каналами, например, Internet. Прямая выгода очевидна: вместо дорогостоящих междугородних или международных каналов используется стандартный и более дешевый канал. На рисунке показана организация связи двух локальных сетей через Internet.



Использование протокола PPTP для связи двух локальных сетей через Internet.

Для защиты канала PPTP применяет алгоритмы шифрования Password Authentication Protocol и Challenge Handshake Authentication Protocol. Кроме того, PPTP позволяет использовать Internet как основную магистраль для сетей NetBEUI или IPX за счет инкапсуляции и шифрования PPP-пакетов. Так что виртуальная корпоративная сеть не обязательно должна работать только по TCP/IP.

Для установки фильтрации PPTP вызовите в **Control Panel** диалоговое окно конфигурирования протокола TCP/IP, выберите вкладку **Properties** и щелкните кнопку **Advanced**. В появившемся диалоговом окне потметьте флажок **Enable PPTP Filtering**.



Внимание: Выбрав фильтрацию PPTP для сетевой платы, Вы тем самым запрещаете этой плате использование любых других сетевых протоколов. Пример такого режима работы — компьютер с несколькими установленными сетевыми платами, одна из которых (с активизированной фильтрацией PPTP) подключена к Internet, а остальные — к локальной сети. Внешние клиенты смогут получить доступ по PPTP к этому компьютеру, а значит, и к корпоративной сети.

Обеспечение безопасности при удаленном доступе

Система защиты Windows NT Server интегрирована с RAS. Учетные записи пользователей любого домена могут применяться удаленными пользователями для доступа. Во время соединения аутентификация может шифроваться.

Доменная основа защиты

Серверы удаленного доступа, использующие доменную модель защиты Windows NT Server, либо группируются в одном домене, либо распределяются по нескольким доменам, между которыми можно установить доверительные отношения.

Централизованные домены

Размещение всех серверов удаленного доступа в одном домене упрощает централизованное администрирование, так как при этом надо работать только с одной базой бюджетов, что позволяет администратору управлять сразу всеми пользователями и серверами RAS.

Централизованное администрирование не означает, что все серверы должны физически находиться в одном месте. Так как домен — логическая структура, серверы могут реально располагаться в разных местах, но при этом принадлежать к одному домену.

Если в подразделениях свои собственные учетные записи пользователей, установите доверительные отношения, но серверы удаленного доступа будут управляться централизованно. Принадлежность всех серверов RAS к одному домену позволяет управлять несколькими серверами одновременно.

Не обнаружив пользователя в том домене, где находится сам, сервер удаленного доступа ищет его во всех доверяемых доменах и принимает первый отклик. Если отклик приходит из домена, в котором у данного пользователя другой пароль или нет привилегии удаленного доступа, то аутентификации не происходит, даже если в другом домене пользователь обладает привилегией удаленного доступа.

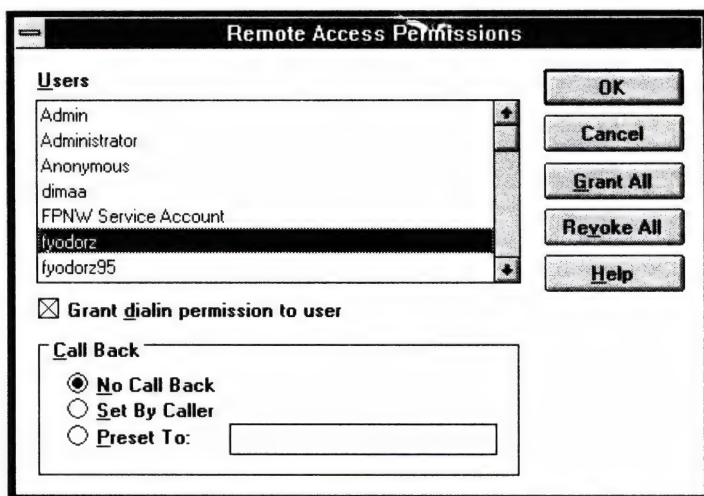
Распределенные домены

В небольших организациях, где важно локальное управление, или в организациях без централизованной системы защиты в каждой группе могут быть свои домены удаленного доступа. Для взаимодействия между ними установите доверительные отношения, сгруппировав в одном домене или распределив между несколькими функции защиты.

Привилегия удаленного доступа

Чтобы подключиться к сети через сервер удаленного доступа, пользователь должен обладать привилегией удаленного доступа. Она предоставляется командой **Permissions** из меню **Users** в программе **Remote Access Admin**. Можно предоставить эту привилегию сразу всем бюджетам домена (щелкнув кнопку **Grant All**) или отдельным пользователям (выбрав нужное имя в списке и пометив флажок **Grant dialin permission to user**).

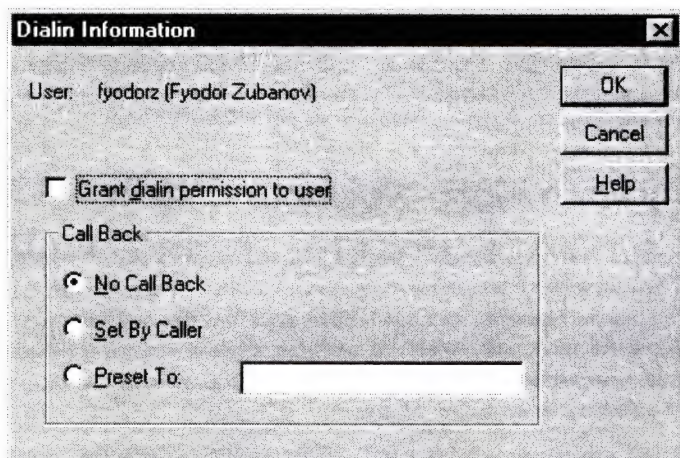
В защищенных системах, естественно, не следует предоставлять удаленного доступа бюджету **Guest**.



Диалоговое окно Remote Access Permissions.



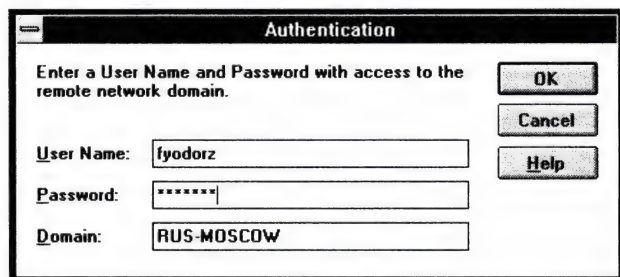
- В Windows NT 4.0 есть и более тонкий способ предоставления привилегии удаленного доступа, позволяющий назначать или отменять возможность удаленного доступа на этапе создания новой учетной записи пользователя. Кнопка **Dialin** в диалоговом окне **User Properties** раскрывает диалоговое окно **Dialin Information**, в котором можно для данной учетной записи разрешить или запретить удаленный доступ и указать способ его осуществления.



Диалоговое окно Dialin Information.

Аутентификация удаленного доступа

Перед получением доступа в сеть удаленный пользователь должен быть аутентифицирован сервером удаленного доступа. Эта процедура отделена от процесса регистрации на WindowsNT Server. Пароли пользователей и процедура аутентификации шифруются при передаче по каналам связи.



Диалоговое окно Authentication.

Параметры аутентификации (количество попыток, время аутентификации и автоотключение) задаются в реестре. Для их редактирования в редакторе реестра откройте ключ:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
RemoteAccess\Parameters.
```

Число попыток аутентификации

Для ограничения количества неудачных попыток регистрации удаленного пользователя установите значение параметра:

AuthenticateRetries

Тип: REG_DWORD
 Диапазон: от 0 до 10
 По умолчанию: 2

Время аутентификации

Для ограничения времени, в течение которого удаленный пользователь может быть аутентифицирован, установите значение параметра:

AuthenticateTime

Тип: REG_DWORD
 Диапазон: 20 — 600 секунд

Если клиент в течение этого времени не будет аутентифицирован, пользователь автоматически отсоединяется. По умолчанию установлено 120 секунд.

АВТООТКЛЮЧЕНИЕ

Можно установить время неактивной работы, по истечении которого клиент будет автоматически отключен от сервера удаленного доступа. Для этого задайте значение параметра:

AutoDisconnect

Тип: REG_DWORD

Диапазон: 0 — 1000 минут

При соединениях NetBIOS неактивность определяется невозможностью передачи данных NetBIOS (например, копирования файлов, доступа к сетевым ресурсам, отправкой и приемом электронной почты). Если клиенты работают с приложениями, использующими датаграммы NetBIOS, можно установить нулевое значение данного параметра. Если в качестве активного соединения применяется соединение по протоколу NetBEUI, а сервер сконфигурирован для предоставления доступа только к этому компьютеру, значения параметра **AutoDisconnect** игнорируются для всех протоколов.

Нулевое значение параметра деактивизирует функцию автоотключения. По умолчанию установлено 20 минут.

Обратная связь

При подключении к серверу клиента, сконфигурированного для обратной связи, сервер перезванивает клиенту по номеру, который либо предварительно задан на сервере, либо сообщается пользователем при подключении. Это позволяет повысить защищенность системы и исключить случайные звонки. Установление обратной связи указывается при предоставлении привилегии удаленного доступа.

Для этого в диалоговом окне **Remote Access Permissions** программы **Remote Access Admin** выберите одну из опций:

- **Preset To** (предустановлено для);
- **Set By Caller** (устанавливается абонентом);
- **No Callback** (отсутствует — значение по умолчанию).



Примечание: Пока пользователь не идентифицирован и с ним не установлена обратная связь (если выбрана соответствующая опция), никакие данные ни от клиента, ни от сервера не передаются.

Параметром для обратной связи является время, по истечении которого сервер перезванивает клиенту. Для редактирования этого параметра в Редакторе Реестра откройте ключ:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\  
RemoteAccess\Parameters.
```

Время устанавливается параметром:

CallbackTime

Тип:	REG_DWORD
Диапазон:	2 — 12 секунд
По умолчанию:	2 секунды

Этот параметр индивидуален для каждого клиента.

Поддержка защитных хостов

Под защитным хостом подразумевается устройство авторизации, выпускаемое сторонней фирмой и применяемое для проверки прав пользователя на подключение к серверу удаленного доступа. Такая проверка дополняет функции защиты, встроенные в сервер удаленного доступа и Windows NT.

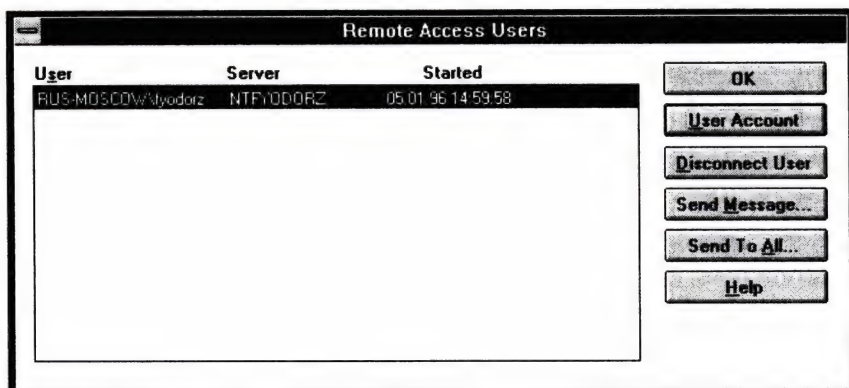
Примером может служить система с двумя устройствами: защитным хостом и карточкой защиты. Защитный хост установлен между модемом и сервером удаленного доступа. Карточка защиты — небольшое, размером с кредитную карточку устройство — похожа на калькулятор без кнопок. Каждую минуту на табло этой карточки появляется уникальный номер доступа, синхронизированный с номерами, рассчитываемыми на защитном хосте. При соединении пользователь посылает номер с карточки на хост. Если номера совпадают, защитный хост пропускает пользователя на сервер удаленного доступа.

Защитный хост нужно сконфигурировать так, чтобы сервер удаленного доступа мог инициализировать модем, не задействовав функций защиты.

Дополнительные рекомендации по использованию защитных хостов содержатся в справке для сервера удаленного доступа.

Отключение пользователей

Утилита **Remote Access Admin** позволяет просматривать всех пользователей, подключенных к выбранному серверу удаленного доступа, и при необходимости отключать их. Отключение выполняется без остановки сервера удаленного доступа и незаметно для других пользователей.



Диалоговое окно Remote Access Users.

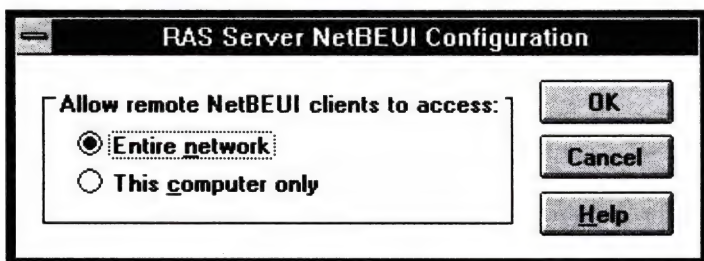
Ограниченный доступ к сети

Используя настройки сети в панели управления, Вы можете:

- ограничить доступ удаленных пользователей к ресурсам сервера удаленного доступа;
- ограничить доступ удаленных пользователей к определенным частям сети.

Предоставление доступа только к серверу

Хотя сервер удаленного доступа можно подсоединить к сети, ограничить доступ удаленных пользователей администратор способен только самим сервером. Это можно указать в настройках сервиса удаленного доступа в панели управления для каждого из протоколов, используемых на сервере. На рисунке показано диалоговое окно ограничения доступа для протокола NetBEUI:



Ограничение доступа к сети по протоколу NetBEUI.

Предоставление доступа только к части сети

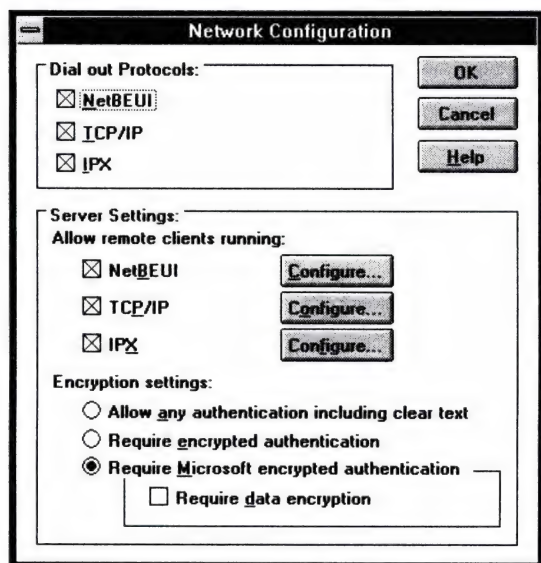
Администратор может ограничить доступ удаленных пользователей к отдельным частям сети, отменив некоторые связи (Bindings) в панели управления. Кроме того, если какие-то сегменты сети применяют различные протоколы, то, запрещая доступ к сети для того или иного протокола, можно запретить доступ к соответствующим сегментам.

Подробная информация о связях приведена в *Windows NT System Guide*.

Шифрование данных

Microsoft RAS применяет шифрование DES, когда и на приемной, и на звонящей стороне используется Windows NT RAS. Клиент RAS может также поддерживать шифрование MD5 (используемый разработчиками PPP-клиентов для шифрования аутентификации) при подключении к серверам удаленного доступа других производителей. При подключении клиентов сторонних фирм сервер Windows NT 3.51 RAS обеспечивает только шифрование DES (но не MD5).

При соединении двух компьютеров, работающих под Windows NT 3.5x, процесс аутентификации всегда шифруется. Аутентификация может выполняться открытым текстом при подключении клиентов сторонних фирм. Параметры шифрования устанавливаются в панели управления при конфигурировании сервиса удаленного доступа.



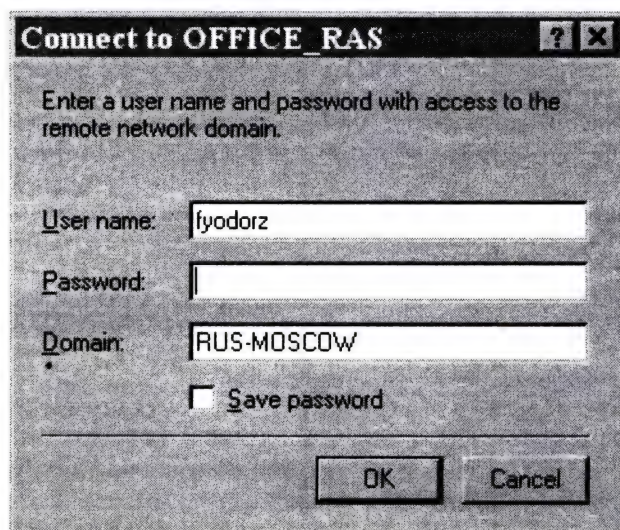
Диалоговое окно *Network Configuration* для сервиса удаленного доступа.

Конфигурирование клиентской части в Windows NT 4.0



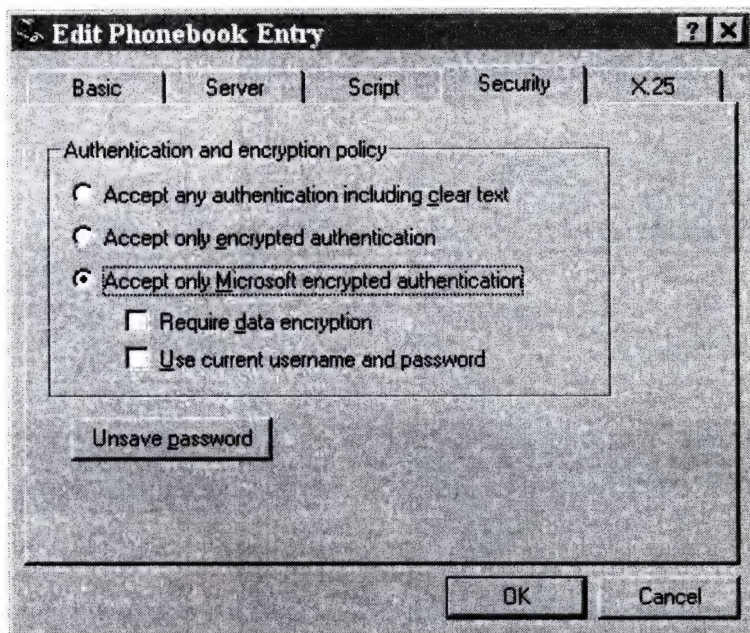
В Windows NT 4.0 появился ряд функций, которые, с одной стороны, упрощают построение глобальных сетей на базе RAS, а с другой — могут негативно сказаться на защищенности системы. Начнем с неприятного.

Если в Windows NT 3.5x для регистрации в удаленной сети использовались имя и пароль, отличные от имени и пароля пользователя, зарегистрировавшегося на клиентской машине, то непосредственно перед началом соединения необходимо было указать нужные имена. Это было не очень удобно для пользователя, однако гарантировало защиту от несанкционированного доступа по RAS. В четвертой версии пользователю достаточно отметить флажок **Save Password** во время первой регистрации в удаленной сети, чтобы его об этом больше никогда не спрашивали. Несомненно, это удобно в работе. Щелкнул ярлык — и пошел процесс дозвола и соединения с удаленным сервером. Но здесь очень велик риск, что в Ваше отсутствие на рабочем месте (а Вы, скажем, еще пренебрегли моими советами по защите компьютера) посторонний так же легко и просто войдет в сеть предприятия или попутешествует за Ваш счет по Internet.



Диалоговое окно *Connect to...*

Если уж так получилось и Вы сохранили пароль, то, одумавшись, “забудьте” его. Для этого в настройках конкретной записи в телефонной книги (диалоговое окно **Edit Phone Book Entry**) выберите вкладку **Security** и щелкните кнопку **Unsave Password**.



Диалоговое окно *Edit Phonebook Entry*:

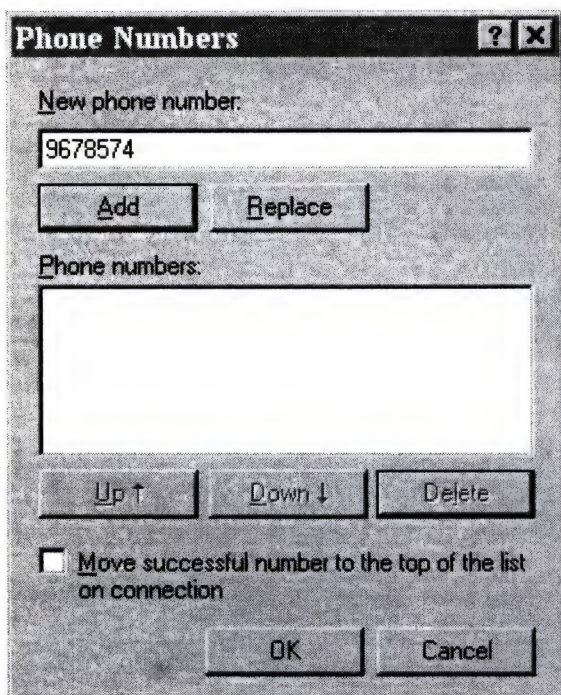
Да, и не забудьте, подключаясь к серверу Windows NT, установить опцию **Accept Only Microsoft Encrypted Authentication**, которая сделает невозможным “перехват” пароля.

Теперь о приятном.

Выбор альтернативного номера

Наверняка Вы сталкивались с такой ситуацией: Вы пытаетесь подключиться к корпоративной сети, чтобы отправить почту или узнать последние детали заключаемого контракта, а телефон занят. Проклиная все на свете, Вы в сотый раз набираете номер... А вот теперь можно указать несколько альтернативных номеров для дозвола. Более того, номера можно расположить по степени важности (или надежности линии, или ее скорости). И если занят первый номер, система переключится на второй, потом на третий и т.д.

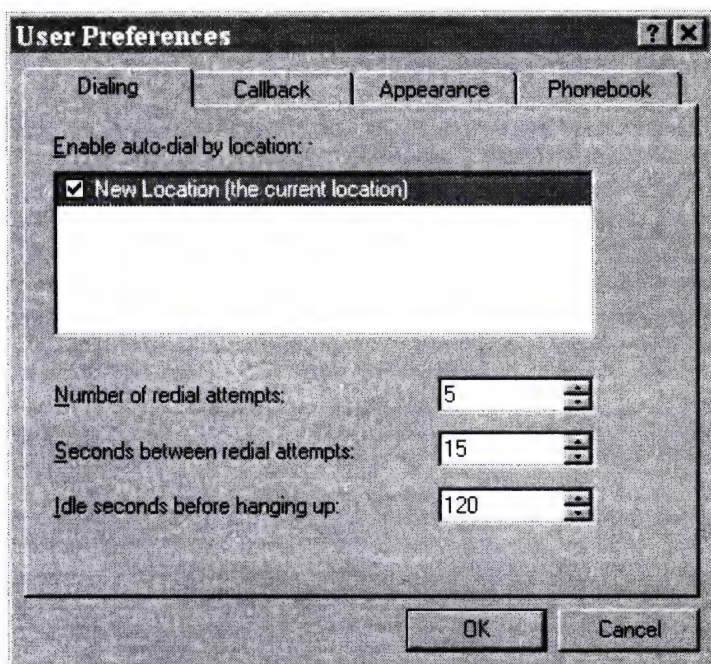
- Если при этом отмечен флажок ***Move successful number to the top of the list on connection***, то номер, по которому удастся соединиться, будет перенесен в начало списка.



- *Список альтернативных номеров.*

Возобновление связи

- Частенько связь обрывается во время работы. Допустим, Вы сделали запрос к базе данных, ждете ответа, и тут раздается предательский сигнал: линия "приказала долго жить"! Вот тут-то и понадобится такая функция, как автоматическое возобновление связи.



Конфигурация параметров автоматического возобновления связи.

Вы можете указать число попыток возобновления (по умолчанию 5), время между попытками (по умолчанию 15 секунд) и время бездействия, по истечении которого Вы будете отключены от сервера. Но помните: на сервере есть аналогичный параметр, и то, что Вы установили на клиентской машине время большее, чем на сервере, не является основанием полагать, что Вас не отключат раньше.

Кстати, описанная функция тесно связана с возможностью Подключения по требованию. Когда приложение пытается обратиться к ресурсу, недоступному в локальной сети, но имеющемуся в удаленной, система автоматически предложит связаться по модему с удаленной сетью.

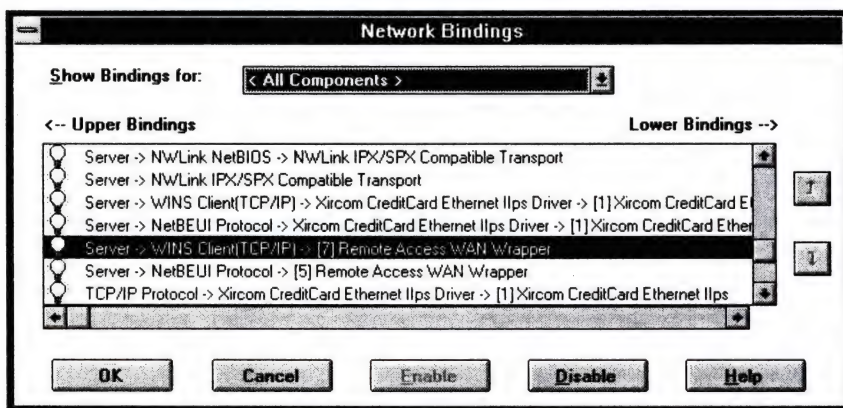
Доступность информации об удаленном доступе

- Настраивая общие параметры связи для пользователя, можно определить ряд таких, которые влияют на внешнее проявление деятельности клиента удаленного доступа. К ним относятся:

<i>Параметр</i>	<i>Описание</i>
Preview Phone Numbers before dialing	Если этот флажок отмечен, пользователю доступны номера набираемых телефонов. Для обеспечения конфиденциальности не отмечайте его.
Show location Setting before dialing	Этот параметр существует для мобильных пользователей: в новом городе или стране им будет проще разобраться с местными телефонными кодами.
Start Dial-up Networking Monitor before Dialing	Запускает монитор состояния модема перед началом дозвона. В зависимости от настроек монитор изображается в отдельном окне или на панели задач.
Show connection progress while dialing	Отображает процесс подключения и аутентификации на экране.
Close on dial	Диалоговое окно Dial-up Networking закрывается при удачном соединении.
Use wizard to create new phonebook entries	Создает новые записи в телефонной книге с помощью программы-мастера. Удобно для неопытных пользователей, слабо разбирающихся в вопросах защиты сети.
Always prompt before auto-dialing	Если выбран этот параметр, у пользователя будет запрашиваться подтверждение всякий раз при возобновлении (или установлении по требованию) связи. В системах, выполняющих роль маршрутизатора между двумя локальными сетями, отмечайте его.

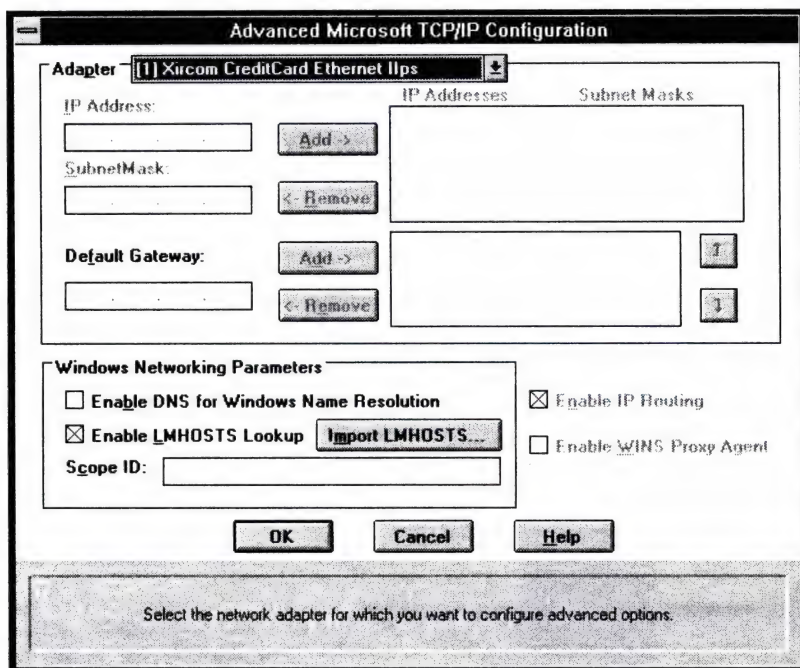
Предоставление одностороннего доступа в Internet

Первая часть проблемы решается стандартными приемами, большинство которых описано в этой книге: хорошие пароли, жесткая бюджетная политика, ограничение членов административной группы, применение NTFS и ограничение прав доступа, выполнение только действительно необходимых сервисов, жесткие права доступа к каталогам, предоставляемым в совместное использование, аудит. Кроме того, отделите некоторые сервисы от сетевых адаптеров. Допустим, в компьютере установлены две сетевые платы, причем одна подключена к Internet, другая — к внутренней сети. Во внутренней сети компьютер выполняет серверные функции, в Internet — только клиентские. В этом случае зайдите в панель управления и в разделе **Network** выберите **Bindings**. Далее деактивизируйте сервис **Server** на плате, подключенной к Internet.



Диалоговое окно *Network Bindings* в *Control Panel*.

Если во внутренней сети используется протокол TCP/IP, запретите маршрутизацию между сетевыми адаптерами на этом компьютере для фильтрации сетевых пакетов, приходящих извне. С этой целью сбросьте флажок **Enable IP Routing** в диалоговом окне **Advanced Microsoft TCP/IP Configuration** в настройках сети в панели управления.



Диалоговое окно Advanced Microsoft TCP/IP Configuration.

Дополнительно на компьютере — шлюзе в Internet — советую установить защитное программное обеспечение, предоставляющее доступ определенным пользователям локальной сети к ресурсам Internet и одновременно отсекающее доступ из Internet в локальную сеть. Пример такого программного обеспечения — Microsoft Internet Access Server.

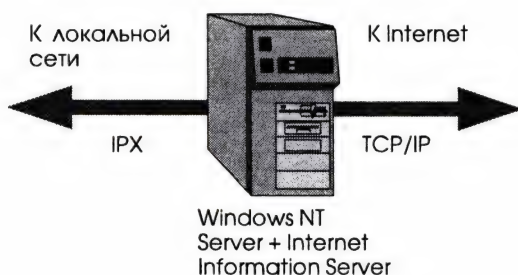
Часть локальной сети как ресурс Internet

Допустим, в Вашей локальной сети имеется сервер Web, доступ к которому осуществляется из Internet, а администрирование — из локальной сети. Доступ из Internet к другим ресурсам сети, естественно, должен быть закрыт. “А что опасного в этом Internet, вокруг которого так много шума?” — спросите Вы. Дело в том, что кроме “цивилизованных” пользователей, в Internet есть и “дикари”,

которые только и мечтают о том, чтобы взломать чужую сеть и уничтожить шутки ради данные на незащищенных серверах. Рассказывают, одна небольшая компания, установив свой Web-сервер и подключив его к Internet, объявила о его существовании, не приняв никаких мер защиты. Увы, на следующий день после подключения сотрудники не обнаружили на своем сервере ни одного файла! Кто, когда и как это сделал, остается тайной, окутанной мраком.

Как же защитить сервер от вторжения? Одно из решений этой задачи — Microsoft Internet Information Server (IIS), включающий в себя защищенные серверы Web, FTP и Gopher.

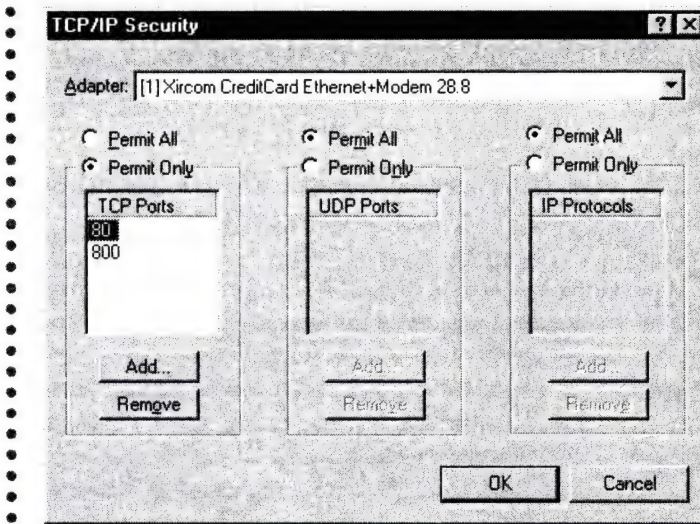
Особенностью IIS является независимость его консоли администратора (**Internet Service Manager**) от типа используемого протокола. Поэтому можно развязать Internet и локальную сеть по протоколам, а на том сервере, где установлен IIS, принять обычные для Windows NT меры защиты.



Как показано на рисунке, локальная сеть может быть связана с сервером по протоколу IPX, в то время как к Internet он будет подключен по протоколу TCP/IP, что надежно разделит сети. Чтобы подобным образом сконфигурировать сервер, свяжите соответствующие протоколы с разными сетевыми адаптерами в диалоговом окне Network Bindings в панели управления.

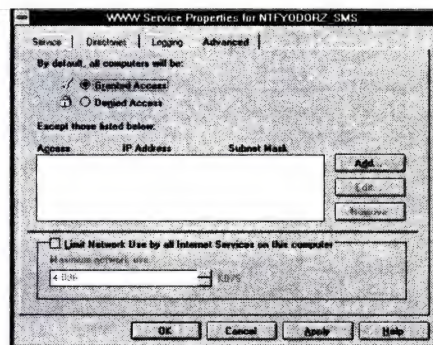
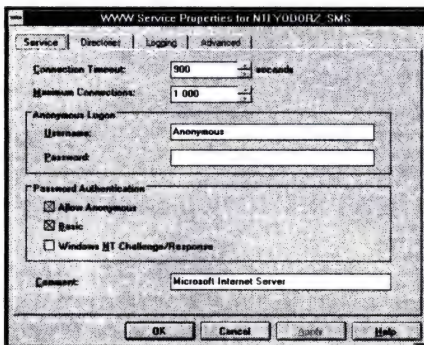


- По умолчанию NT Server предоставляет доступ ко всем портам TCP, UDP
- и протоколам IP. В Windows NT 4.0 есть дополнительная возможность
- ограничения доступа. Вызвав в **Control Panel** диалоговое окно настроек
- протокола TCP/IP и щелкнув кнопку **Advanced**, в появившемся диалого-
- вом окне Вы обнаружите флажок **Enable Security**. Отметив его и щелкнув
- кнопку **Configure**, Вы попадете в диалоговое окно **TCP/IP Security**. Здесь
- можно указать, к каким портам TCP или UDP компьютера и по каким
- протоколам IP возможен внешний доступ. Это очень полезное свойство.
- Предположим, Ваш сервер является сервером WWW в Internet и одновременно — сервером файлов в локальной сети. Тогда, ограничив возможно-
- сти доступа для сетевой платы, подключенной к Internet, Вы обезопасите
- свою сеть от нежелательного вторжения.



Диалоговое окно TCP/IP Security.

Если пользователям Internet предоставляется информация на Web или ином сервере, доступ к ней необходимо ограничить. Это достигается средствами самого информационного сервера. Например, в IIS можно задействовать несколько степеней защиты: простую защиту по нешифрованному паролю, шифрованный пароль, механизм защиты Windows NT, запрет доступа к серверу определенным пользователям или группам (определяется по адресу IP и маске) и механизм SSL (Secure Sockets Layer). Определенную роль играет и предоставление одному и тому же серверу разных имен.



Возможности ограничения доступа в Microsoft Internet Information Server.

В общем случае процесс предоставления доступа можно описать следующей схемой.

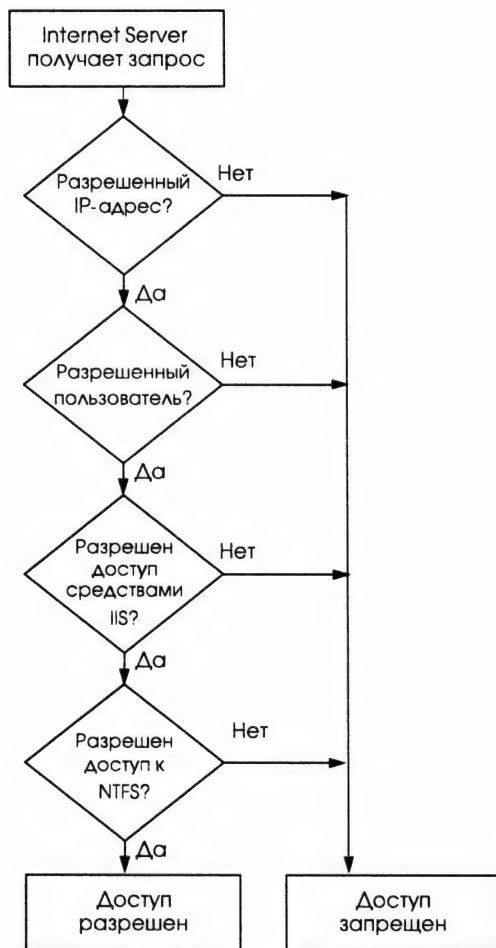


Схема предоставления доступа к ресурсам Internet Information Server.

Таким образом, только комплексное использование всех средств защиты, предоставляемых как самой операционной системой, так и дополнительными продуктами, может уберечь Вашу сеть от вторжения "прекрасного и яростного" мира, называемого Internet.

Использование реестра

Все мы еще помним MS-DOS — относительно простую операционную систему, конфигурирование которой выполнялось несколькими командами, вводимыми в текстовых файлах AUTOEXEC.BAT и CONFIG.SYS. Появление Windows и OS/2 привело к заметному росту количества команд в этих файлах и увеличению числа дополнительных. Каждая программа, устанавливаемая в системе, считала своим долгом создать свой конфигурационный файл. Это, естественно, самым плачевным образом сказывалось на надежности работы системы в целом. В Windows NT используется новое, единое место хранения инициализационных параметров — реестр (Registry).



Назначение реестра

В Windows 3.x запуск системы, соединение с сетью и выполнение приложений требуют многочисленных файлов конфигурации с некоторой формой синхронизации между ними. Операционная система Windows NT сохраняет и проверяет информацию конфигурации только в одном месте — реестре.

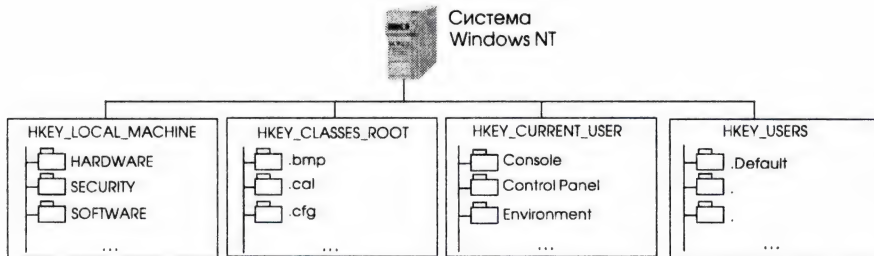
- *Программа установки* (Windows NT Setup) или другие программы установки приложений или аппаратных средств всякий раз при выполнении добавляют в реестр новые данные о конфигурации. Например, новая информация добавляется при установке нового SCSI-адаптера или изменении параметров видеоплаты.
- *Программа распознавания* каждый раз при запуске компьютера под Windows NT помещает данные о конфигурации аппаратных средств в реестр. Эта информация включает список аппаратных средств, обнаруженных в системе.
- *Ядро Windows NT* в процессе запуска системы извлекает из реестра различную информацию о драйверах устройств и порядке их загрузки.
- *Драйверы устройств* посылают и получают параметры загрузки и данные конфигурации из реестра. Эти данные подобны тем, что записывались в строках DEVICE= в файле CONFIG.SYS в MS-DOS. Драйвер устройства должен сообщать об используемых им ресурсах системы. Приложения и драйверы могут считывать эту информацию Реестра для обеспечения интеллектуальной установки и конфигурации программ.
- *Административные инструментальные средства* Windows NT (например, предоставляемые в панели управления и находящиеся в группе программ **Administrative Tools**) используются для изменения данных конфигурации.

Для просмотра содержимого реестра предназначена специальная программа — редактор реестра Registry Editor. Чтобы ее запустить, выполните REGEDT32.EXE.

Структура реестра

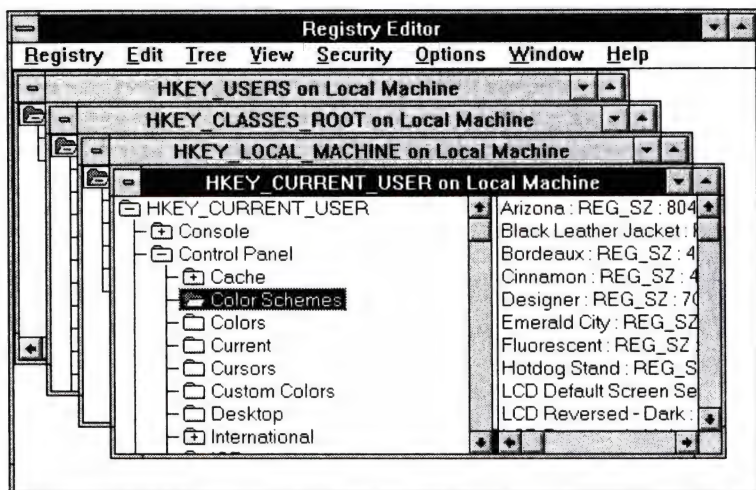
Реестр структурирован как набор четырех поддеревьев ключей, содержащих базы данных с информацией о компьютере и пользователях. Информация о компьютере включает сведения об аппаратных средствах и программном обеспечении, установленном на компьютере.

В реестре Windows NT каждый индивидуальный ключ может содержать элементы данных, называемые *значимыми элементами*, и дополнительные *подключи*. В структуре реестра ключи аналогичны каталогам, а значимые элементы — файлам.



Четыре поддерева в реестре Windows NT.

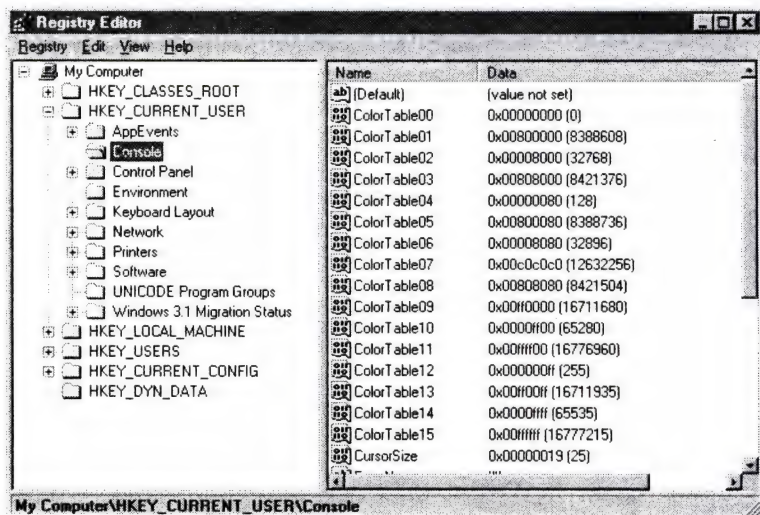
Поддевео	Описание
HKEY_LOCAL_MACHINE	Содержит информацию о локальной компьютерной системе, включая аппаратные средства и данные операционной системы, такие как тип шины, системная память, драйверы устройств и данные управления запуском.
HKEY_CLASSES_ROOT	Содержит данные связи и внедрения объектов (OLE) и данные ассоциации файловых классов.
HKEY_CURRENT_USER	Содержит профиль текущего зарегистрированного пользователя, включая системные переменные, персональные группы программ, настройки рабочего стола, сетевые соединения, принтеры и приложения.
HKEY_USERS	Содержит все активно загруженные профили пользователя, включая HKEY_CURRENT_USER, который всегда связан с порождением из HKEY_USERS, и профиль по умолчанию. Пользователи, обращающиеся к серверу дистанционно, в этом ключе на сервере не имеют профилей; их профили загружаются в реестр на собственных компьютерах.
HKEY_CURRENT_CONFIG	Содержит информацию о текущей конфигурации компьютера (только в Windows NT 4.0).
HKEY_DYN_DATA	Динамические данные о системе (только в Windows NT 4.0).



Редактор реестра Registry Editor.



- В Windows NT 4.0 редактор реестра изменился: его внешний вид стал точно таким, как и в Windows 95. Соответственно изменилось и исполнение некоторых функций. Вместо четырех поддеревьев, изображаемых в разных окнах, все ключи изображаются в виде единого дерева, с шестью главными ветвями:



Редактор реестра в Windows NT 4.0.

Ульи и файлы

Реестр разделен на части — *ульи*. Они названы так разработчиками по аналогии с ячеистой структурой пчелиного “жилья”. Улей — это дискретный набор ключей, подключей и значений, находящийся вверху иерархии реестра. Улей поддерживается одиночным файлом и файлом .LOG, находящимися в каталоге %systemroot%\system32\config. Ниже перечислены все ульи для компьютера, работающего под управлением Windows NT.

<i>Улей реестра</i>	<i>Имя файла</i>
HKEY_LOCAL_MACHINE\SAM	SAM, SAM.LOG
HKEY_LOCAL_MACHINE\SECURITY	SECURITY, SECURITY.LOG
HKEY_LOCAL_MACHINE\SOFTWARE	SOFTWARE, SOFTWARE.LOG
HKEY_LOCAL_MACHINE\SYSTEM	SYSTEM, SYSTEM.ALT
HKEY_CURRENT_USER	USER###, USER###.LOG или ADMIN###, ADMIN###.LOG
HKEY_USERS\DEFAULT	DEFAULT, DEFAULT.LOG

Целостность и восстановление улья в реестре

Реестр гарантирует целостность индивидуальных действий, т.е. любое одиночное изменение значения для установки, удаления или сохранения будет работать или не работать, даже если система отключается из-за сбоя питания, отказа аппаратных средств или проблем с программным обеспечением. Например, если приложение устанавливает значения для двух элементов (А и Б), возможна одна из следующих ситуаций:

- присвоено новое значение элементу А или элементу Б;
- присвоены новые значения элементам А и Б;
- не сделано никаких изменений.

Благодаря целостности индивидуальных действий исключена ситуация получения разрушенной смеси старых и новых значений для элемента. Например, не будет получена разрушенная смесь старого и нового элемента А. Кроме того, ключ, содержащий элементы А и Б, будет иметь размер, временную метку и другие данные, не противоречащие фактическому состоянию ключа.

Данные записываются в реестр при сбросе данных, который происходит через несколько секунд после изменения данных или когда приложение преднамеренно сбрасывает данные на жесткий диск. Выполняется следующий процесс сброса для всех ульев:

1. Все измененные данные заносятся в файл LOG улья вместе с картой их расположения в улье, а затем выполняется сброс на диск файла LOG. В этот момент принимается, что все измененные данные записаны в файл LOG.
2. Первый сектор файла улья маркируется для указания, что файл находится в переходном состоянии.
3. Измененные данные записываются в файл улья.
4. Файл улья маркируется как завершенный.



Кстати: При аварийном отказе системы между пунктами 2 и 4 при следующей загрузке улья в процессе запуска (если это не улей профиля, загружаемый при входе в систему) система видит метку, установленную в пункте 2, и продолжает восстановление улья с учетом изменений файла LOG. Таким образом, файлы LOG не используются, если улей не в переходном состоянии. В противном случае улей не может быть загружен без файлов LOG.

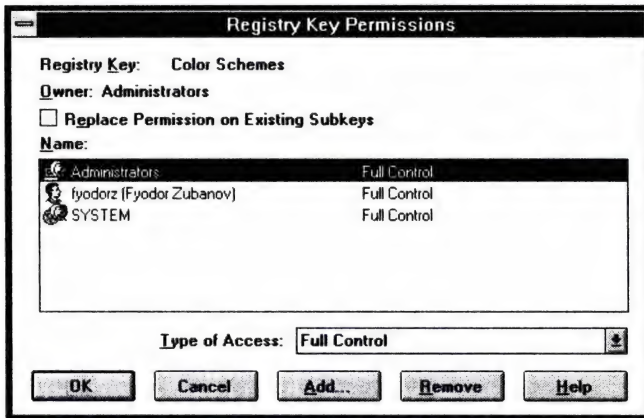
Несколько иной процесс заполнения применяется для улья SYSTEM. Этот важный элемент для запуска системы используется слишком рано в процессе запуска, поэтому восстановить его описанным способом нельзя.

Файл SYSTEM.ALT содержит копию данных файла SYSTEM. В процессе заполнения изменения маркируются, записываются и затем отмечаются как выполненные; затем тот же процесс заполнения повторяется для файла SYSTEM.ALT. При сбое питания, отказе аппаратных средств или проблемах с программным обеспечением на любой стадии описываемого процесса один из файлов SYSTEM или SYSTEM.ALT будет содержать правильную информацию.

Ограничение доступа к реестру

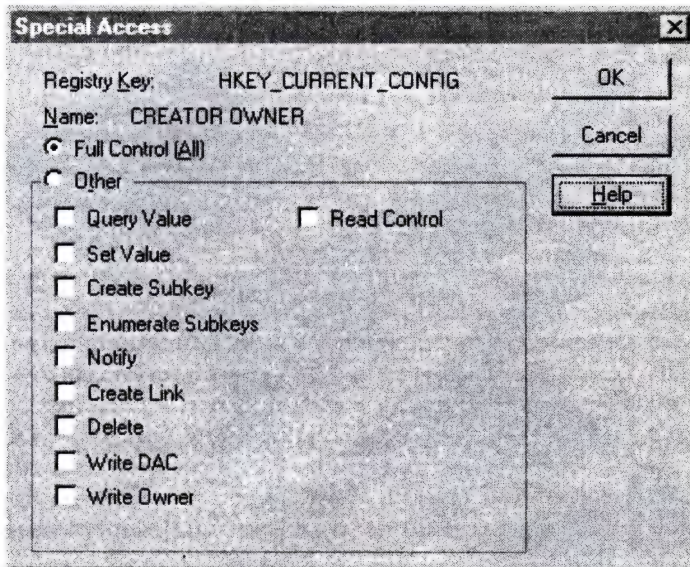
Самый простой способ защитить редактор реестра и файлы реестра — разместить их на разделе NTFS с ограничением доступа средствами файловой системы. Это гораздо проще, чем ограничить доступ к отдельным элементам реестра.

Но если файлы реестра размещены на FAT, права доступа (по умолчанию они зависят от поддерева) можно установить с помощью самого редактора реестра. Для доступа к диалоговому окну разграничения доступа к реестру выберите из меню **Security** команду **Permissions**.



Диалоговое окно *Registry Key Permissions*.

Вид этого диалогового окна во многом аналогичен диалоговым окнам разграничения доступа к файлам, принтерам и т.п. Можно назначить доступ только на чтение, полный либо специальный. При назначении специального вида доступа появляется диалоговое окно ***Special Access***.



Диалоговое окно *Special Access* в редакторе реестра.

К специальным видам доступа относятся:

- | | |
|----------------------|--|
| Query Value | Право чтения значения ключа в реестре. |
| Set Value | Право вводить значения в реестр. |
| Create Subkey | Право создавать подключи выбранного ключа. |

Enumerate Subkeys	Право находить подключи указанного ключа в реестре.
Notify	Право уведомлять.
Create Link	Право создания символьной ссылки на выбранный ключ.
Delete	Право удалять выбранный ключ.
Write DAC	Право доступа к ключу с целью записи списка контроля доступа.
Write Owner	Право доступа к ключу с целью вступления во владение им.
Read Control	Право доступа к информации о защите ключа

Использование реестра для быстрого восстановления конфигурации 32-разрядных приложений

Информацию о своей конфигурации приложения Win32 сохраняют в реестр. Как правило, эта информация заносится в поддерево HKEY_CURRENT_USER\Software. Следующим ключом будет имя фирмы (например, Microsoft) или общий тип приложения (например, VB and VBA program Settings). Зачастую, установив приложение на новый компьютер, необходимо быстро восстановить ту же конфигурацию, что и на эталонном компьютере. Естественно, подобные настройки (скажем, внешний вид и расположение панелей инструментов, цвета окон и текста, рабочие каталоги, используемые дополнительные утилиты и т.п.) можно выполнить средствами самого приложения, но это займет довольно много времени. Для быстрого копирования конфигурации легче переносить содержимое поддереьев и значений с одного компьютера на другой.

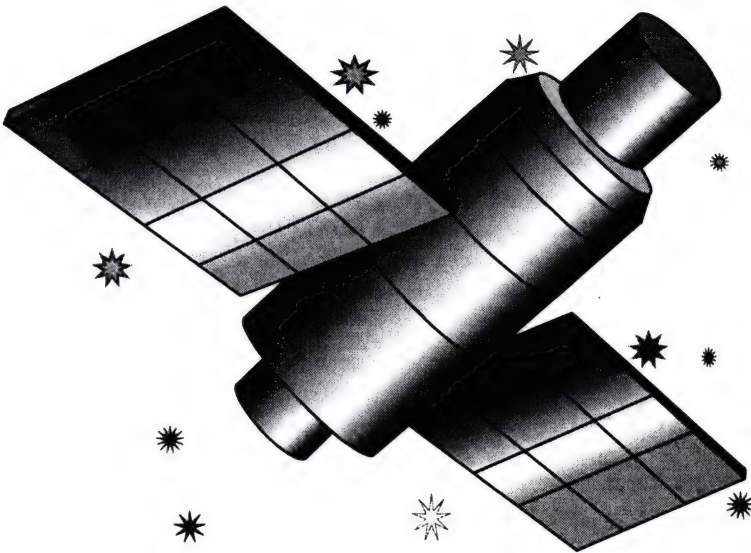
Прежде чем выполнить перенос, сохраните ключ реестра в файл. Для этого, выбрав в меню **Registry** команду **Save Key**, укажите имя файла. Затем на компьютере-приемнике выберите в реестре корневой для вновь конфигурируемого приложения ключ. Если приложение уже установлено, то, как правило, соответствующий ему подключ будет прописан в реестре. Если же его нет, создайте. Далее выделите требуемый подключ и, выбрав команду **Restore** в меню **Registry**, укажите ранее сохраненный файл. Если Вы обладаете соответствующими правами доступа к этому ключу в реестре, он будет полностью заменен на значения эталонного ключа, включая все возможные подключи. Запуск приложения сразу покажет, что информация была успешно скопирована.



Замечание: Перед переносом значений ключей убедитесь, что переносимая конфигурация не противоречит параметрам Вашего компьютера. Например, если переносится указание о том, что рабочим каталогом является E:\winnt40\win32\myapp, такой каталог должен существовать на компьютере-приемнике.

Аудит и мониторинг системы

Возможно, встретив малознакомое слово, Вам захочется пропустить эту часть. Не спешите. Когда в Вашей системе вирус уничтожит ценную информацию или Вы заподозрите ее утечку к конкурентам, будет поздно рвать волосы и горестно вопрошать, как это могло случиться. Позаботьтесь об этом заранее и предоставьте системе возможность последить за тем, что в ней творится, и сообщить Вам обо всем подозрительном. Не пренебрегайте аудитом.



Аудит в Windows NT

Аудит в сетях Windows NT включает в себя системные элементы просмотра, мониторинга и документирования, а также оценки защиты информационных ресурсов. Под термином "защита" подразумевается *целостность, конфиденциальность, доступность и неразрывность* информации. Он относится и к физическому имуществу, технике, операционным системам и т.д., принадлежащим компании, но используется для определения легальности функций корпорации.

- *Целостность* означает, что данные и программы изменяются только в соответствии с правильно авторизованными действиями и обработкой.
- *Конфиденциальность* означает, что корпоративные данные доступны только правильно авторизованному персоналу.
- *Неразрывность* означает, что данные, однажды сохраненные на сетевом носителе, изменяются только при правильно авторизованных действиях и обработке.
- *Доступность* означает, что данные, программы и техника всегда доступны для авторизованных пользователей сети.

В соответствии с этим в Windows NT имеется возможность регистрации и отображения:

- пользователей, получивших доступ к объекту;
- типа попытки доступа;
- того, был ли доступ успешным или нет.

Для доменов все регистрируемые события записываются в журнал регистрации событий защиты на контроллере домена и относятся к событиям, произошедшим либо на контроллере, либо на всех серверах домена. На рабочих станциях все регистрируемые события заносятся в журнал регистрации событий защиты рабочей станции.



Примечание: По умолчанию только администраторы обладают привилегией **Manage Auditing and Security Log** (Управление аудитом и журналом регистрации защиты).

Журналы регистрации событий защиты можно просмотреть, выбрав из меню **Log** утилиты **Event Viewer** команду **Security**.

Windows NT обеспечивает аудит на уровне системных событий и на объектном уровне для доступа к файлам и каталогам. Первый уровень устанавливается в **User Manager** любым пользователем с привилегией **Manage Auditing and Security Log**. Второй определяется в **File Manager**. Также могут регистрироваться события, связанные с изменениями в реестре и изменениями параметров принтеров.

АУДИТ СИСТЕМНЫХ СОБЫТИЙ

Аудит включается командой **Audit** в меню **Policies в User Manager** или в **User Manager for Domains**; в диалоговом окне укажите события, которые будут регистрироваться (**Audit this Events**). Если опция **Audit this events** не выбрана, аудит полностью отключен.



Примечание: По умолчанию аудит отключен. Однако настоятельно рекомендуется его использовать.

Если выбрана опция **Do Not Audit**, то отключены как аудит на системном уровне, так и аудит файлов и каталогов. В противном случае можно указать конкретный тип события, подлежащего регистрации, а также только удачные результаты события, только неудачные, либо и те и те.

Audit Policy		
Domain: MOW-DEMO-M		
<input type="radio"/> Do Not Audit <input checked="" type="radio"/> Audit These Events:		
	Success	Failure
Logon and Logoff	<input type="checkbox"/>	<input checked="" type="checkbox"/>
File and Object Access	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Use of User Rights	<input type="checkbox"/>	<input checked="" type="checkbox"/>
User and Group Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security Policy Changes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Restart, Shutdown, and System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Process Tracking	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: OK, Cancel, Help

Диалоговое окно *Audit Policy*.

В таблице описаны системные события, которые могут быть зарегистрированы.

<i>Категория</i>	<i>Регистрируемые события</i>
Logon and Logoff	Попытки регистрации, выхода из системы, создания и удаления подключений к серверам. Содержится информация о типе регистрации и о том, была ли она удачной. Для сокращения записей в журнале рекомендуется регистрировать только неудачные попытки регистрации и выхода из системы.
File and Object Access	Доступ к файлу или каталогу, регистрация которых установлена в File Manager , а также использование принтера, управляемого компьютером. Для сокращения записей в журнале рекомендуется регистрировать только неудачные попытки доступа.
Use of User Rights	Удачное использование привилегий пользователей, неудачные попытки применения привилегий, не назначенных пользователям. Предоставляется некоторая информация о том, когда некоторые специальные привилегии были назначены (но не о том, когда они использовались). Для сокращения записей в журнале рекомендуется регистрировать только неудачные попытки использования привилегий.
User and Group Management	Создание, удаление или изменение учетных записей пользователей и групп, таких как User Created или Group Membership Change .
Security Policy Changes	Предоставление или отмена привилегий для пользователей и групп. Установление или отмена доверительных отношений между доменами.
Restart, Shutdown and System	Выключения и перезагрузки компьютера, заполнение журнала регистрации событий и очистка записей в журнале регистрации при его переполнении.
Process Tracking	Запуск и остановка процессов в компьютере. Предоставляется подробная информация. Если нет особой необходимости, не стоит отслеживать информацию о процессах, так как это приводит к появлению большого числа записей в журнале и перегружает систему.

Аудит отключен по умолчанию, поэтому каждую из категорий следует включать по отдельности. Конечно, можно регистрировать действия каждого пользователя, события и процессы, но огромное количество относительно простых записей в журнале регистрации затрудняет обнаружение действительно важных — о неудачных попытках. Так что умерьте аппетит и ограничьтесь регистрацией только действительно необходимых событий.

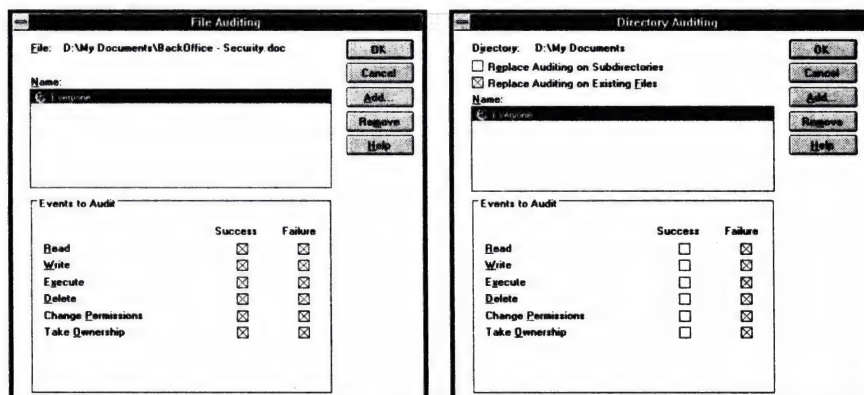


Примечание: Запись регистраций в системе и выходов из нее может порождать огромное число записей в журнале в зависимости от числа пользователей и частоты их регистрации в системе. Рекомендуется выполнить предварительные измерения.

Аудит доступа к файлам и каталогам

Для регистрации доступа к файлам и каталогам используется **File Manager**. Можно регистрировать доступ отдельных пользователей и групп к любому файлу или каталогу.

Выделите в **File Manager** файл или каталог, аудит доступа к которым необходим, а затем в меню **Security** выберите команду **Audit**. В зависимости от того, что выбрано — файл или каталог, — появится диалоговое окно **File Auditing** или **Directory Auditing**.



Диалоговые окна File Auditing и Directory Auditing.

Укажите имена пользователей и групп, доступ которых Вас интересует, и выберите события для регистрации и их тип (успешные/неуспешные). В таблице приведено объяснение категорий:

<i>Доступ к файлу</i>	<i>Доступ к каталогу</i>
Показ данных файла	Показ имен файлов в каталоге
Показ атрибутов файла	Показ атрибутов каталога
Показ владельца файла и прав доступа	Изменение атрибутов каталога
Изменение файла	Создание подкаталогов и файлов
Удаление файла	Удаление каталога
Изменение прав доступа к файлу	Изменение прав доступа к каталогу
Изменение владельца файла	Изменение владельца каталога
Исполнение файла	Показ владельца каталога и прав на доступ

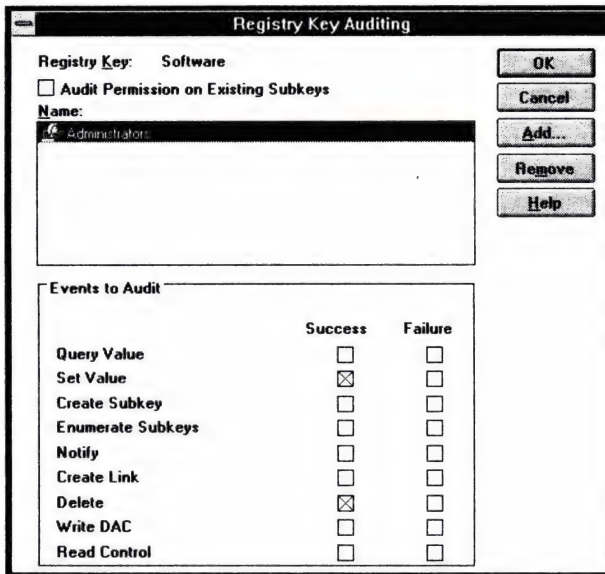
По умолчанию регистрируются события, связанные только с выделенным каталогом и его файлами. Для аудита всех подкаталогов пометьте флажок **Replace Auditing on Subdirectories**. Если установлен и флажок **Replace Auditing on Existing Files**, изменения в аудите будут относиться как к каталогам, так и файлам. В общем случае оба эти флажка должны быть помечены.



Примечание: Для регистрации событий, связанных с файлами и каталогами, в диалоговом окне **Audit Policy** в **User Manager** пометьте флажок **File and Object Access** (подробнее см. выше раздел *Аудит системных событий*).

Аудит реестра

В реестре Windows NT Server содержится информация, относящаяся к защите и аудиту: конфигурация умолчания для файлов журналов регистрации, максимальный размер этих файлов и период хранения данных для каждого из файлов. Аудит реестра устанавливается в редакторе реестра. Можно указать пользователей или группы, для которых будет осуществляться регистрация доступа к выбранным ключам реестра.



Диалоговое окно Registry Key Auditing.

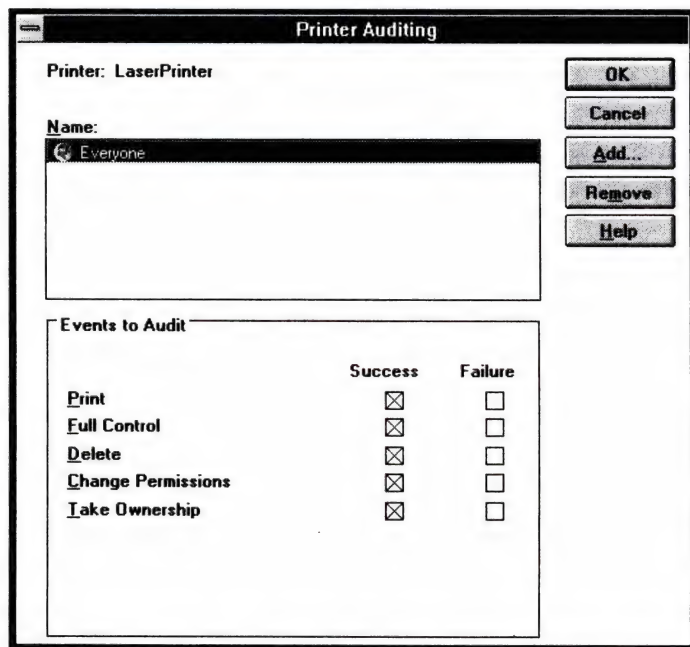
В таблице объясняются опции этого диалогового окна.

Опция	Регистрируемые события
Check Link	События, при которых выполняется попытка открыть ключ с типом доступа Create Link .
Create Subkey	События, при которых выполняется попытка открыть ключ с типом доступа Create Value .
Delete	События, при которых происходит попытка удаления ключа.
Enumerate Subkeys	События, при которых выполняется попытка открыть ключ с типом доступа Enumerate Subkeys (т.е. когда происходит поиск подключа).
Notify	События, при которых выполняется попытка открыть ключ с типом доступа Notify .
Query Value	События, при которых выполняется попытка открыть ключ с типом доступа Query Value .
Read Control	События, при которых идет поиск владельца ключа.
Set Value	События, при которых выполняется попытка открыть ключ с типом доступа Set Value .
Write DAC	События, при которых определяется, кто имеет доступ к ключу.

По умолчанию аудит реестра отключен. Для включения сначала пометьте флажок **File and Object Access** в **User Manager**. Затем в редакторе реестра выберите в меню **Security** команду **Auditing** и укажите события, которые необходимо регистрировать. Аудит каждого ключа и подключа может выполняться индивидуально. Аудит реестра выполняйте от случая к случаю. Напомню: обычно регистрируются только неудачные события, так как регистрация удачных приведет к быстрому переполнению журнала.

Аудит печати

В Windows NT обеспечивается защита печати. Пользователю или группе могут быть предоставлены четыре вида прав доступа к принтеру: **No Access**, **Print**, **Manage Documents** и **Full Control**. Если включена регистрация в меню **Security** в **Print Manager**, можно фиксировать попытки пользователей вывести документ на печать, изменения заданий для печати, приостановки печати, возобновления заданий для печати, перестановки или удаления заданий в очереди на печать. Можно регистрировать и попытки предоставить принтер в совместное использование, удалить принтер, изменить привилегии или владельца.



Диалоговое окно *Printer Auditing*.

По умолчанию сообщение о печати документа посылается его владельцу. Однако он всегда может изменить адресата сообщения о печати в диалоговом окне **Document Details**. Остальным это доступно только при наличии привилегий **Manage Documents** или **Full Control**.

Этот механизм контроля необходимо применять в защищенных системах. Напомню: чтобы изменить адресата данного сообщения, сначала приостановите печать.

Document Details	
Document Title: Notepad - D:\MSOffice\Winword\WDREADME.TXT	
Status:	Pages: 9
Size: 101364	Owner: fyodorz
Printed On: LaserPrinter	Notify: fyodorz
Printed At: 13:27	Priority: 1
Processor: winprint	Start Time: 00:00
Datatype: NT JNL 1.000	Until Time: 00:00

Диалоговое окно Document Details в Print Manager.



Примечание: Для аудита печати пометьте флажок **File and Object Access** в диалоговом окне **Audit Policy** в **User Manager** (подробнее см. выше в разделе *Аудит системных событий*).

Аудит сервера удаленного доступа

В Windows NT Server можно регистрировать деятельность пользователей, подключенных к серверам удаленного доступа (RAS). Единственное отличие пользователя локальной сети от удаленного в том, что последний применяет асинхронную версию сетевого протокола. Мониторинг деятельности удаленных пользователей осуществляется с помощью **Event Viewer**. События, связанные с удаленным доступом, чрезвычайно важны с точки зрения наблюдения защищенности системы.

В приведенных ниже таблицах описаны сообщения, связанные с удаленным доступом.

Записи об успешном использовании RAS

<i>Сообщение</i>	<i>Пояснение</i>
The user <i>имя пользователя</i> has connected and has been successfully authenticated on port <i>имя порта</i>	Указывает на нормальное подключение определенного пользователя к данному порту.
User <i>имя пользователя</i> has disconnected from port <i>имя порта</i>	Указывает на успешное отключение пользователя, инициированное пользователем.

Записи о неуспешном использовании RAS

<i>Сообщение</i>	<i>Объяснение</i>
The user connected to port <i>имя порта</i> has been disconnected because of inactivity.	Линия оставалась бездействующей в течение периода, превышающего значение параметра <i>AutoDisconnect</i> в реестре (подробнее см. главу <i>Использование реестра</i>).
The user has connected and failed to authenticate on port <i>имя порта</i> . The line has been disconnected.	Пользователь ввел неверное имя, пароль или и то и другое. Число неудачных попыток регистрации превысило заданное параметром <i>AuthenticareRetries</i> в реестре (подробнее см. главу <i>Использование реестра</i>).
The user connected to port <i>имя порта</i> has been disconnected because of authentication timeout.	Проверка пользователя заняла больше времени, чем указано. Для изменения периода проверки измените параметр <i>AuthenticateTime</i> в реестре (подробнее см. главу <i>Использование реестра</i>).
The user connected to port <i>имя порта</i> has been disconnected because there was a transport level error during the authentication conversation.	При проверке пользователя произошло слишком много ошибок, возможно из-за зашумленной линии или несовместимости модемов. Попросите пользователя подсоединиться на более низкой скорости.
The user connected to port <i>имя порта</i> has been disconnected because it could not be projected onto the network.	Чаще происходит, если в сети уже имеется рабочая станция с таким именем. Попросите пользователя сконфигурировать компьютер с другим именем или проверьте, не подключен ли он к сети другим способом, например по Ethernet или Token ring.

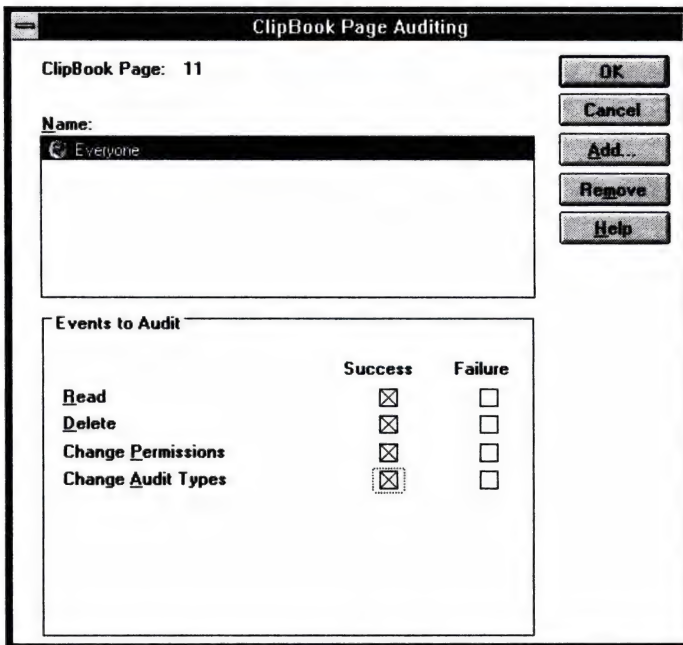
Аудит удаленного доступа должен быть всегда включен.

Аудит Книги обмена

Аудит Книги обмена (*ClipBook*) можно применять для контроля за тем, как пользователи или члены групп работают с совместно используемыми страницами в Книге обмена. Для каждой страницы можно регистрировать как удачные, так и неудачные события. Чтобы установить параметры аудита, нужно быть членом группы **Administrators** или иметь привилегии **Manage Auditing** и **Security Log**. Регистрируемые события заносятся в журнал защиты. Эту функцию следует задействовать только в случае действительной необходимости.

Для аудита страниц Книги обмена выберите нужную страницу, а в меню **Security** — команду **Auditing**; укажите имя пользователя или группы, чьи действия надо регистрировать. Возможен аудит:

- чтения страницы;
- удаления содержимого страницы;
- изменения прав доступа;
- изменения типов аудита.



Диалоговое окно *ClipBook Page Auditing*.



Примечание: Для аудита Книги обмена в диалоговом окне **Audit Policy** в **User Manager** пометьте флажок **File and Object Access** (подробнее см. выше раздел *Аудит системных событий*).

Журналы регистрации событий защиты

В каждом Windows NT Server имеются три журнала для занесения событий, относящихся к системе, защите и приложениям. Заносятся:

- в *системный журнал* — ошибки, предупреждения или информация от системы Windows NT Server;
- в *журнал защиты* — сообщения об удачных и неудачных попытках регистрации, а также события, связанные с использованием ресурсов, такие как создание, открытие или удаление файлов или других объектов;
- в *журнал приложений* — ошибки, предупреждения и информация от выполняемых приложений, таких как электронная почта или СУБД.

Все три журнала хранятся в одном подкаталоге:










```
<systemroot>\system32\config
```

Системный журнал и журнал приложений доступны для просмотра любому пользователю. Журнал защиты могут просматривать только администраторы или пользователи с привилегиями **Manage Auditing** и **Security Log**. Для просмотра журнала защиты выберите в **Event Viewer** команду **Security** из меню **Log**.

Доступ к журналу защиты защищен через список контроля доступа, предоставляющий доступ только администраторам. Журнал защиты должен располагаться на разделе NTFS, чтобы можно было использовать списки контроля доступа. Полное имя файла журнала защиты:

```
<systemroot>\system32\config\secevent.evt
```

У журнала защиты есть заголовок и номер версии, расположенные в начале каждого файла журнала. Заголовок можно использовать, чтобы точно знать, в тот ли журнал заносится информация. Сервис журналирования **Event Log** проверяет существующий файл, прежде чем что-либо в него записать. Если файл ошибочен, сервис **Alert** предупреждает администратора. Когда файл журнала заполнен, при поступлении новой записи администратору посылается предупреждение, а запись в журнал не заносится.

Event Viewer - Security Log on \\NTFYODORZ_SMS					
Log		View	Options	Help	
Date	Time	Source	Category	Event	User
 07.01.96	15:03:35	Security	Detailed Tracking	593	fyodorz
 07.01.96	15:03:29	Security	Privilege Use	577	SYSTEM
 07.01.96	15:03:29	Security	Privilege Use	577	fyodorz
 07.01.96	15:03:22	Security	Detailed Tracking	592	fyodorz
 07.01.96	14:59:35	Security	Object Access	562	SYSTEM
 07.01.96	14:59:18	Security	Object Access	562	SYSTEM
 07.01.96	14:58:18	Security	Detailed Tracking	593	fyodorz
 07.01.96	14:58:18	Security	Detailed Tracking	592	fyodorz
 07.01.96	14:58:08	Security	Detailed Tracking	592	fyodorz

Журнал регистрации событий защиты в Event Viewer.

Дважды щелкнув любое из событий в списке, Вы получите о нем более подробную информацию.

Event Detail

Date: 07.01.96 **Event ID:** 592
Time: 14:58:18 **Source:** Security
User: fyodorz **Type:** Success Audit
Computer: NTFYODORZ_SMS **Category:** Detailed Tracking

Description:
A new process has been created:
New Process ID: 4288577568
Image File Name: WINFILE.EXE
Creator Process ID: 4289395552
User Name: fyodorz
Domain: MDW-DEMO-M
Logon ID: (0x0.0x1134)

Data: ☒ Bytes ☐ Words

Close Previous Next Help

Подробная информация о событии.

При показе события и подробной информации отображается также информация из заголовка журнального файла. События могут быть отсортированы по элементам заголовка. В таблице приведены описания параметров заголовка:

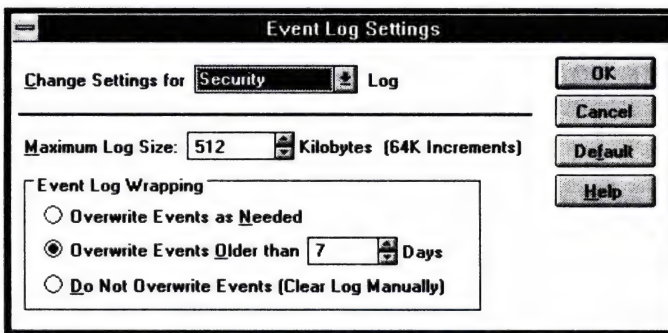
<i>Элемент заголовка</i>	<i>Значение</i>
Date	Дата, когда произошло событие.
Time	Время, когда произошло событие.
Source	Имя системы, породившей событие. Для записей сообщений защиты это всегда Security .
Category	Классификация события источником событий. Например, к категориям защиты относятся Logon и Logoff , Policy Change , Privilege Use , System Event , Object Access , Detailed Tracking и Account Management .
Event ID	Уникальный идентификатор события, зависящий от модуля.
User	Трансляция SID субъекта, породившего событие, в имя бюджета. Это имя является олицетворением ID-клиента, если субъект олицетворяет клиент, или же имя первичного ID, если не олицетворяет.
Computer	Имя компьютера, на котором порождено событие.
Event Type (Только в режиме подробного просмотра)	Указывает, была ли попытка удачной или неудачной в зависимости от того, был ли установлен аудит удачных или неудачных попыток.

Дополнительно к перечислению по их идентификатору события в журнале защиты перечислены по категориям. В таблице приведены категории событий и их значения:

<i>Категория</i>	<i>Значение</i>
Account Management (Управление пользователями и группами)	Описывают высокоуровневые изменения в базе учетных записей пользователей, такие как создание новой учетной записи или изменение членства в группе. Возможно также выполнение более подробного аудита на объектном уровне.
Detailed Tracking (Отслеживание процессов)	Предоставляют подробную информацию об отслеживании субъектов. Сюда включена такая информация, как активизация программы, повторение указателя на программу и неявный доступ к объекту.
Logon/Logoff (Регистрация и выход)	Описывают однократные попытки регистрации или выхода из системы и степень успешности. В описание каждой попытки регистрации входит указание на тип запрашиваемой или выполненной регистрации: интерактивная, сетевая или регистрация сервиса.

Категория	Значение
Object Access (Доступ к файлам и объектам)	Описывают как удачные, так и неудачные попытки доступа к защищенным объектам.
Policy Change (Изменения в политике защиты)	Описывают высокоуровневые изменения в политике защиты, такие как назначение привилегий или возможностей регистрации. Возможно также выполнение более подробного аудита на объектном уровне.
Privilege Use (Использование привилегий пользователя)	Описывают как удачные, так и неудачные попытки использования привилегий. В журнал также включается информация о том, когда были назначены некоторые специальные привилегии. Эти специальные привилегии регистрируются только при назначении, а не во время использования.
System Event (Изменения в политике защиты)	Указывают на что-то затрагивающее защищенность всей системы в целом или при записи в журнал.

Для каждого их журналов регистрации администратор может указать такие параметры, как максимальный размер файла журнала и как поступать при переполнении журнала.



Определение параметров журнала.

Регистрация событий начинается на этапе загрузки. Если в диалоговом окне **Audit Policy** в **User Manager** отмечены все флажки, включая **Process Tracking**, Windows NT может занести в журнал огромный объем информации, и журнал быстро переполнится. Как только это произойдет, система остановится. В Windows NT есть возможность указать, как поступить в этом случае, чтобы система не встала. По умолчанию на каждый журнал отводится 512 Кб. Но этот размер можно увеличить в соответствии с объемом диска и памяти. Администратор не может сделать журнал меньше существующего — сначала журнал надо очистить.

В каждой организации должны быть установлены правила архивирования журналов регистрации. Архивирование совместно с опциями заполнения журнала позволяет обеспечить сохранность всех зарегистрированных системных событий и предотвратить переполнение журнала и остановку системы.

В таблице перечислены опции заполнения журнала и их объяснение:

<i>Опция заполнения</i>	<i>Значение</i>
Overwrite Events as needed	Если выбрано это значение, то при переполнении журнала новые записи будут замещать старые. Установлена по умолчанию.
Overwrite Events Older than x Days	Эту опцию лучше всего использовать при регулярном архивировании журнала. По умолчанию устанавливается 7 дней.
Do not Overwrite Events	Гарантирует сохранность всех записей. Требуется ручная очистка журнала.

Чтобы система не останавливалась при переполнении журнала, установите в реестре флажок:

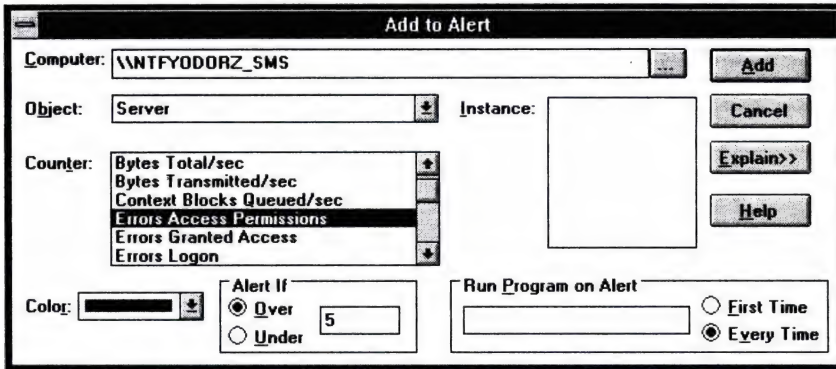
```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\
Control\Lsa\CrashOnAuditFail
```

Если этот флажок установлен и система по какой-либо причине не может сделать запись в журнал, система остановится. Если он не установлен, то при переполнении журнала система выдаст сообщение администратору: *"The Security Log file is full"*.

Сигналы тревоги (Alerts)

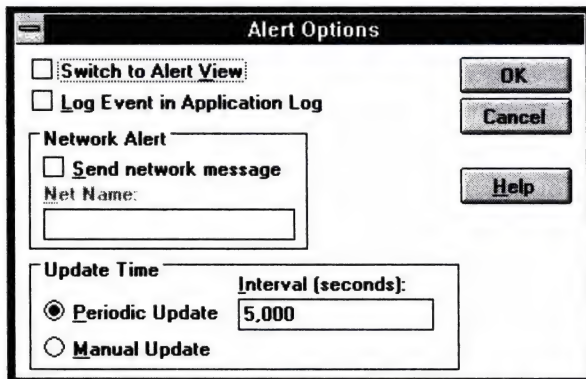
Windows NT Server может рассылать сообщения о тревоге определенным пользователям. Эти сообщения могут быть связаны и с событиями, затрагивающими безопасность системы, например, превышение числа неудачных попыток регистрации.

Для указания рассылаемых сигналов тревоги и выбора пользователей, которым это сообщение будет разослано, используется **Performance Monitor**. Выбрав в нем команду **View Alert**, администратор указывает в списке необходимые сигналы, а также условия, при которых они вырабатываются. Для каждого из таких сигналов можно задать приложение или командный файл, который будет выполняться в условиях наступления события.



Диалоговое окно Add To Alert.

Определив сигналы тревоги, можно установить их общие параметры. В частности, указать пользователей, которым будет посылаться данный сигнал или заставить **Performance Monitor** автоматически переключаться в режим просмотра сигналов тревоги. Использовать эту возможность настоятельно рекомендуется.



Диалоговое окно Alert Options в Performance Monitor.

Допустим, Ваш сервер является почтовым узлом, на котором хранится вся почтовая поступающая к Вам корреспонденция. Сервер работает в автономном режиме в удаленном помещении. Согласно установленной в Вашей организации политике, вся почта, полученная более чем 2 месяца назад, удаляется с сервера. Кроме того, объем жесткого диска не так велик, и надо постоянно следить, чтобы свободного пространства хватало для размещения новой почты. Для соблюдения всех этих требований можно использовать **Performance Monitor**.

Add to Alert

Computer: \\NTFYODORZ-M [Add]

Object: LogicalDisk [v]

Instance: 0 ==> C:
0 ==> D:

Counter: % Disk Read Time
% Disk Time
% Disk Write Time
% Free Space
Avg. Disk Bytes/Read
Avg. Disk Bytes/Transfer

Color: [v]

Alert If
☐ Over
☒ Under 5

Run Program on Alert
 Deloldmail.cmd -Z
☐ First Time
☒ Every Time

Counter Definition
 Percent Free Space is the ratio of the free space available on the logical disk unit to the total usable space provided by the selected logical disk drive

[Add] [Cancel] [Explain>>] [Help]

Опишите в нем сигнал тревоги, возникающий при уменьшении объема свободного пространства на диске менее определенной величины (**LogicalDisk, %Free Space, Under 5%**); укажите программу, которая будет удалять (или архивировать на стример) всю почту, возраст которой превышает 2 месяца. Так как эта операция должна выполняться каждый раз при наступлении описанных условий, отметьте переключатель **Every Time**. Задав все параметры, "нажмите" кнопку **Add**.

Этим, однако, конфигурация сигнала тревоги не заканчивается. Наверное, нет смысла проверять объем свободного пространства на диске каждые 5 секунд. В нашем примере достаточно ограничиться 1 часом. Кроме того, такие события необходимо заносить в журнал для регистрации и оповещать администратора сети. Поэтому выставьте общие параметры вот так:

Alert Options

☐ Switch to Alert View [OK]

☒ Log Event in Application Log [Cancel]

Network Alert
☒ Send network message
 Net Name: \\ntfyodorz [Help]

Update Time
☒ Periodic Update Interval (seconds): 3600
☐ Manual Update

Анализ и настройка производительности сервера с помощью программы Performance Monitor

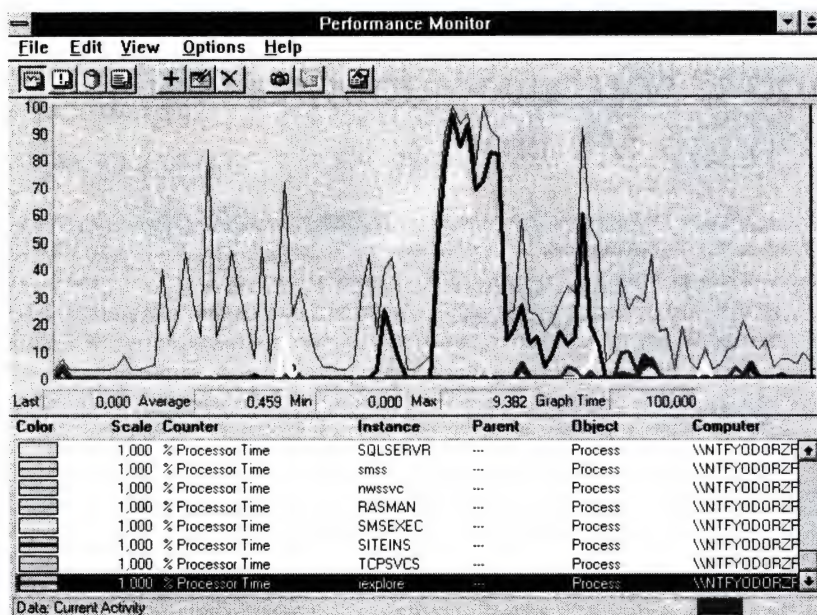
Порой, работая с сервером, Вы замечаете его необъяснимую, на первый взгляд, “задумчивость”. То замедляется перекачка файлов по сети, то запрос к базе данных выполняется гораздо медленней, чем обычно. Можно, конечно, глядя в монитор, помедитировать и погадать о причинах такого поведения. Но лучше пойти другим путем — запустить монитор производительности (**Performance Monitor**). Выше мы говорили, как его использовать для отслеживания некоторых критических ситуаций и генерации сигналов тревоги. Это лишь одна из его функций.

Не менее важной функцией является отслеживание загруженности отдельных процессов, потоков, устройств и т.п. практически в реальном масштабе времени. Загруженность (или иной параметр) отображаются в виде диаграммы. На одной странице можно наложить кривые, соответствующие различным измеряемым величинам, а затем, сопоставив их, сделать вывод о том, что именно в большей степени повлияло на перегрузку сервера.

Сразу после установки сервера Вы можете контролировать разнообразные параметры, относящиеся к сервисам операционной системы: **Browser**, **Server**, **Redirector**, а также параметры, характеризующие работу отдельных систем: процессора, памяти, жесткого диска и т.п. Запуск любого приложения сопровождается порождением новых процессов и потоков. Влияние каждого из них на общую загруженность системы также можно оценить с помощью **Performance Monitor**.

В дальнейшем установка новых серверных приложений приводит к добавлению в список контролируемых параметров новых элементов, описывающих работу установленных приложений. Например, установка Microsoft Internet Information Server приводит к появлению таких объектов, как **FTP Server**, **Gopher Server**, **HTTP Server** и **Internet Information Services Global**. Каждый из них имеет большое количество измеряемых параметров.

На рисунке показан пример анализа работы сервера, на котором установлены Microsoft SQL Server 6.0, Systems Management Server 1.1, Internet Information Server 1.0, DHCP- и WINS-серверы. Также эта машина выполняет роль шлюза в сеть Netware и имитирует работу сервера Netware.

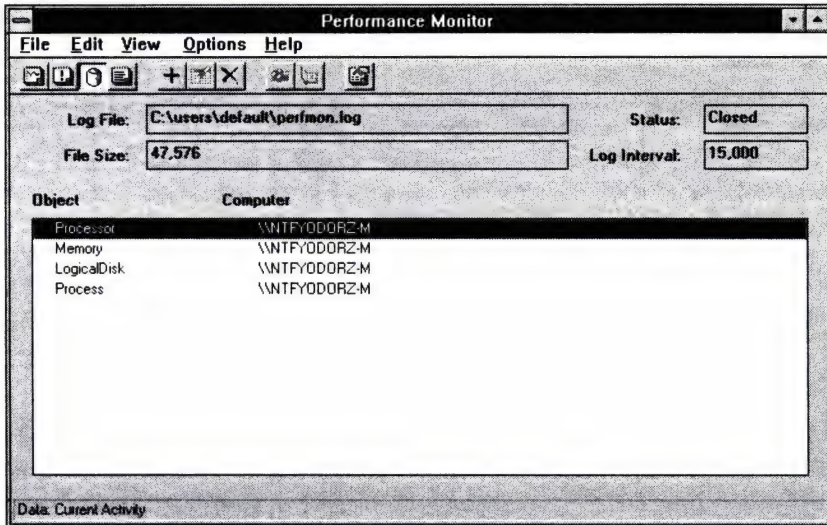


Окно Performance Monitor.

В интервал времени, показанный на рисунке, проводилась переконфигурация Systems Management Server (SMS). Среди параметров, отображенных на диаграмме, выделяются два: общая загрузка процессора (тонкая линия) и загрузка процессора, связанная с выполнением переконфигурации SMS (толстая линия в центре диаграммы). Анализ кривых показывает, что в первой половине данного отрезка времени процессор был загружен исполнением некоторых процессов, не включенных в рассмотрение (это могли быть процессы, инициированные пользователями по сети). Далее загрузка процессора очень четко коррелирует с процессом переконфигурирования SMS. И, наконец, по завершении его вновь доминируют процессы пользователей: обращение к серверу Web и SQL Server.

При выполнении анализа нет никакой необходимости неотрывно смотреть на экран и ждать, когда же произойдет то событие, что приведет к ограничению производительности сервера. Вместо этого просто перенаправьте поток дан-

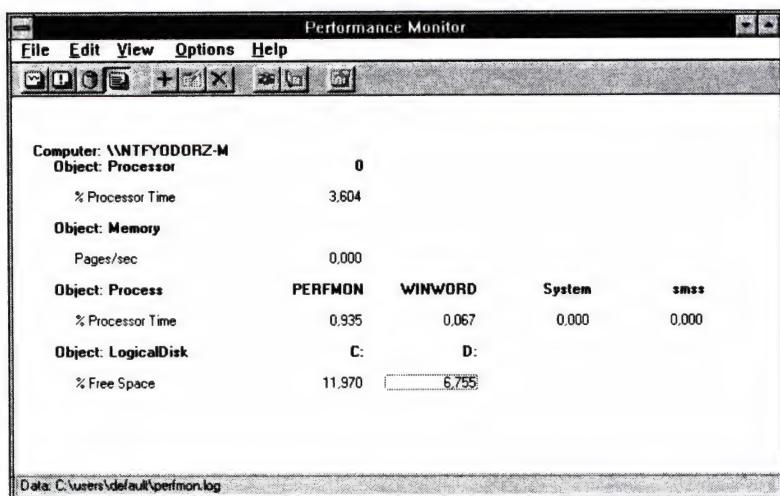
ных в журнал. При конфигурировании журнала можно указать имя файла журнала, интервал обновления и объекты, информация о которых будет фиксироваться. Такой способ анализа удобен, например, в случае тонкой настройки производительности сети.



Окно *Performance Monitor* в режиме заполнения журнала.

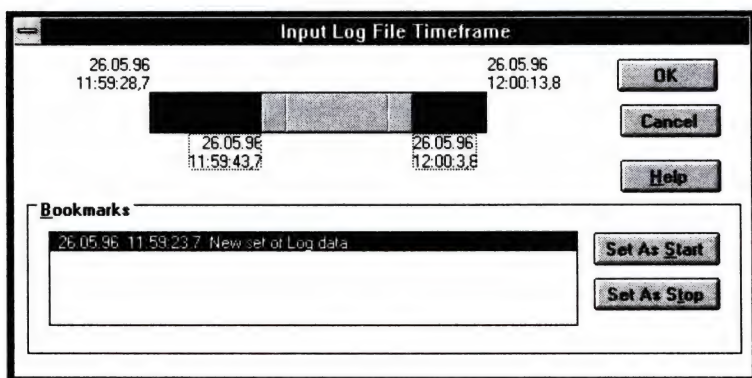
Проанализировать информацию, занесенную в журнал, можно потом несколькими способами. Во-первых, представить в виде диаграммы, подобной рассмотренной выше. Для этого, переключившись в режим просмотра диаграммы (**View Chart**), выберите в меню **Options** команду **Data From** и укажите имя файла журнала. После этого останется лишь указать интересующие параметры для каждого из занесенных в журнал объекта. На диаграмме сразу будет отражена деятельность в системе на момент регистрации в журнале.

Второй способ представить информацию из журнала — оформление ее в виде отчета (**Report**). Для этого переключитесь в режим просмотра отчетов и, выбрав в меню **Options** команду **Data From**, укажите имя файла журнала. Затем добавьте к отчету интересующие значения.



Окно Performance Monitor в режиме просмотра отчетов.

При взгляде на отчет, показанный на рисунке, сразу возникает вопрос: а к какому интервалу времени он относится? Чтобы это понять или указать иной интервал, выберите в меню **Edit** команду **Time Window** и укажите начальную и конечную точки регистрации на слайдере:



Установка интервала времени в Performance Monitor.

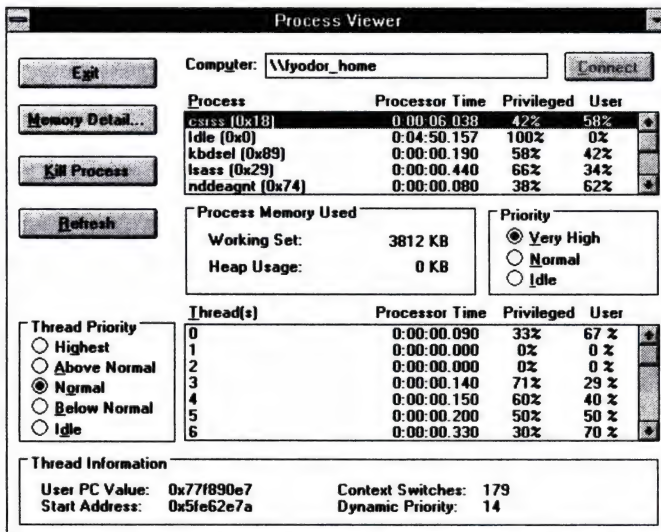
Поиск и терминирование отдельных процессов

Иногда при анализе загрузки сервера выясняется, что сервер загружен чем-то непонятным. Вы закрываете все приложения, отключаете от сервера всех пользователей, но кривая, соответствующая занятости процессора, указывает на интенсивную работу. В этом случае необходимо проанализировать запущенные в системе процессы. Бывает, при некорректном завершении какого-либо при-

ложения ряд процессов, соответствующих этому приложению, остается активным в памяти. Попытка обнаружить их в списке задач не дает желаемого результата, так как задача в целом уже снята. Процессы выявляются с помощью монитора производительности. Для анализа выбирается объект **Process**, а на график выносятся все “подозрительные экземпляры” (Instances) объектов. Обнаружив процесс, влияние которого на загрузку процессора очевидно, проверьте, не системный ли он, и прекратите (терминируйте) его.

Нежелательные процессы можно прекратить разными способами:

1. Выйдите из системы и зарегистрируйтесь в ней снова. Этот способ идеально “убивает” процессы, порожденные Вашей персональной деятельностью. К достоинствам этого способа относится непрерывность работы сервера и терминирование всех несистемных процессов. К недостаткам — возможность остановки только тех процессов, что порождены пользователем, зарегистрировавшимся локально.
2. Перезагрузите систему. Это, пожалуй самый эффективный, но и самый “кровавый” способ, пригодный для использования на рабочей станции или сервере небольшой рабочей группы, но никак не на сервере подразделения.
3. Воспользуйтесь утилитой **PVIEWER** из *Windows NT Resource Kit* — она позволяет не только увидеть все процессы в системе, но и при необходимости терминировать любой из них. Достоинство данного способа — непрерывность работы сервера и терминирование любого, отдельно взятого процесса. Однако при этом администратору необходимо прекрасно знать имена всех системных процессов, чтобы случайно их не уничтожить.



Программа Pviewer.

4. Воспользуйтесь утилитами **TLIST** и **KILL**, также входящими в поставку *Windows NT Resource Kit*. Работа с этими программами аналогична работе с **PVIEWER** за тем исключением, что они имеют неграфический интерфейс. **TLIST** сообщает имена и идентификаторы всех процессов, активных в системе, а **KILL** позволяет "убить" процесс по его идентификатору. Эти утилиты особенно полезны в том случае, если Вы администрируете удаленный сервер и подключились к нему в терминальном режиме с использованием утилиты Telnet.

4.0

5. В Windows NT 4.0 имеется встроенная возможность просмотра активных процессов и их терминирования. Для этого используется **TaskList**, который, кроме исполняемых задач, показывает и процессы, а также ресурсы, выделяемые под каждый из процессов. Для остановки процесса достаточно выделить его в списке и щелкнуть кнопку **End Process**.

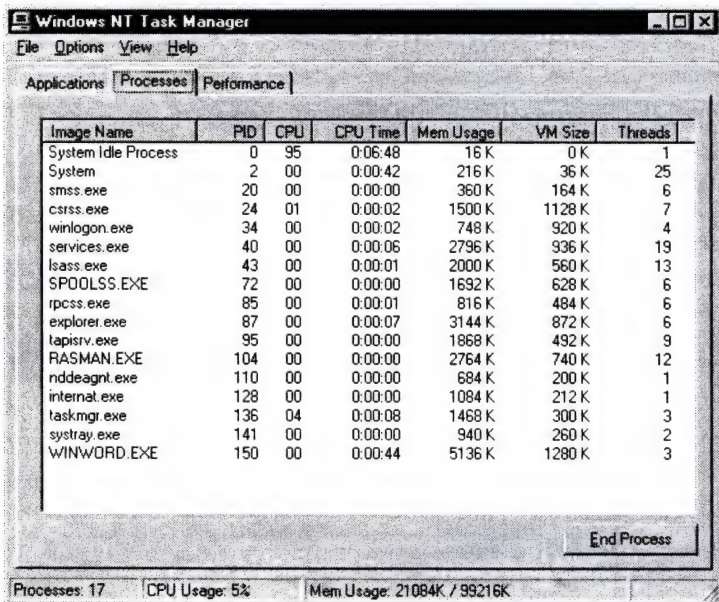


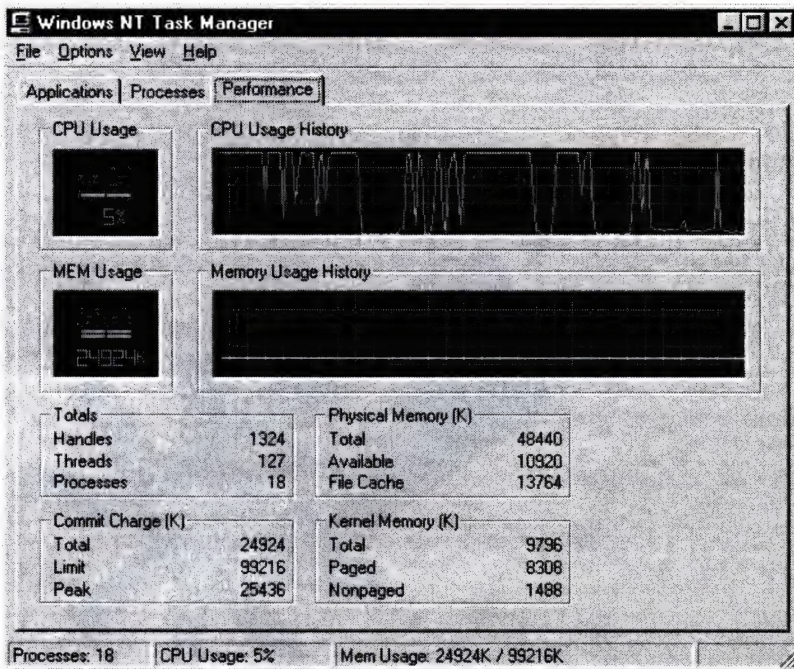
Image Name	PID	CPU	CPU Time	Mem Usage	VM Size	Threads
System Idle Process	0	95	0:06:48	16 K	0 K	1
System	2	00	0:00:42	216 K	36 K	25
smss.exe	20	00	0:00:00	360 K	164 K	6
csrss.exe	24	01	0:00:02	1500 K	1128 K	7
winlogon.exe	34	00	0:00:02	748 K	920 K	4
services.exe	40	00	0:00:06	2796 K	936 K	19
lsass.exe	43	00	0:00:01	2000 K	560 K	13
SPOOLSS.EXE	72	00	0:00:00	1692 K	628 K	6
rpcss.exe	85	00	0:00:01	816 K	484 K	6
explorer.exe	87	00	0:00:07	3144 K	872 K	6
lapisrv.exe	95	00	0:00:00	1868 K	492 K	9
RASMAN.EXE	104	00	0:00:00	2764 K	740 K	12
nddeagnt.exe	110	00	0:00:00	684 K	200 K	1
internat.exe	128	00	0:00:00	1084 K	212 K	1
taskmgr.exe	136	04	0:00:08	1468 K	300 K	3
systray.exe	141	00	0:00:00	940 K	260 K	2
WINWORD.EXE	150	00	0:00:44	5136 K	1280 K	3

Окно Task Manager в режиме просмотра процессов

Анализ загрузки системы в Windows NT 4.0

В Windows NT версии 4.0 появилась возможность экспресс-контроля загрузки системы. Можно, не вызывая монитора производительности, оценить в реальном масштабе времени использование ресурсов центрального процессора и памяти, посмотреть количество потоков, открытых файлов, распределение памяти между ядром системы и приложениями, а также ряд других полезных параметров. Все, что нужно — запустить **Task Manager** и открыть в нем вкладку **Performance**.

Понятно, что данный инструмент не обеспечивает всей гибкости и возможностей, предоставляемых **Performance Monitor**, но удачно дополняет его функции в плане оперативности получения наиболее часто используемой информации.



Окно **Task Manager** в режиме графического представления загрузки процессора.

Приложения

Итак, книга прочитана, и Вас распирают знания о грамотном администрировании системы. Вам не терпится реализовать на практике прочитанное. Секунду! Быть может, не все, что Вы знаете, пригодится в конкретной ситуации. Возможно, чем-то можно пренебречь ради достижения наивысшей производительности. В этих приложениях содержатся практические рекомендации по настройкам Windows NT Server, обеспечивающим различную степень надежности, — выберите самую подходящую.



Установки, обеспечивающие минимальную защиту

Вы можете не задумываться о защите компьютера, если в нем не хранится важная информация или он расположен в защищенном помещении. Если надо, Windows NT позволяет сделать систему полностью доступной, без какой-либо защиты.

Требования физической защиты

Примите все меры предосторожности для предотвращения кражи важного оборудования. Проще говоря, запирайте комнату, в которой стоит компьютер, в отсутствие сотрудников или прикрепите блоки компьютера к стене гибким кабелем. Можно установить порядок выноса компьютера или отдельных его частей из помещения, чтобы ни один элемент не пропал "случайно".

Используйте специальные устройства для защиты компьютера и периферии от перенапряжения. Регулярно проверяйте диск и дефрагментируйте его для выявления сбойных секторов и обеспечения высшей производительности.

Требования программной защиты

Для обеспечения минимальной защиты не используются никакие функции Windows NT. Фактически можно разрешить автоматическую регистрацию административного бюджета (или любого другого бюджета), следуя рекомендациям, приведенным в главе 12 "Configuration Management and the Registry" в *Windows NT Resource Guide*. Это позволит любому, имеющему физический доступ к компьютеру, включить его и сразу получить доступ к системным ресурсам.

По умолчанию доступ ограничен несколькими файлами. Для обеспечения минимальной защиты предоставьте группе **Everyone** доступ ко всем файлам.

Следует принять антивирусные меры, так как вирусы могут нарушить работу Ваших программ, либо использовать незащищенный компьютер для проникновения в другие системы.

Установки, обеспечивающие обычную защиту

Чаще всего компьютеры используются для хранения важных или ключевых данных. Это могут быть финансовые данные или архивы персональной корреспонденции. Хочется защитить компьютер и от преднамеренных или случайных изменений в его параметрах. При всем том пользователи не должны преодолевать барьеры на пути к ресурсам, с которыми они работают.

Требования физической защиты

Как и в случае минимальной защиты, компьютер должен быть защищен как любое чувствительное оборудование. В общих чертах это означает хранение машины в недоступном для посторонних помещении, каким обычно является офис или дом. Иногда есть смысл прикрепить компьютер к стене кабелем. Если у него имеется замок, храните ключ в безопасном месте. Правда, если ключ потеряется, даже авторизованный пользователь не сможет работать.

Требования программной защиты

Защита системы требует усилий как со стороны администратора, устанавливающего программное обеспечение, так и со стороны повседневных пользователей — они должны воспитывать в себе привычку выходить из системы по окончании рабочего дня и запоминать (а не записывать) пароли.

Предупреждение при регистрации

Перед регистрацией пользователя в системе в WindowsNT возможен вывод на экран сообщения, определяемого пользователем. Во многих организациях это сообщение предупреждает о легальности работы. Отсутствие такого предупреждения может рассматриваться как приглашение войти в систему без каких-либо ограничений.

Это предупреждение может также инструктировать пользователя о том, как ввести имя и пароль.

Подробнее о конфигурировании сообщения см. раздел *Предупреждение о легальности использования*.

Учетные записи пользователей и группы

Для обеспечения стандартной защиты требуется использование учетных записей пользователей (имен пользователей) и паролей. Подробнее о создании и работе с учетными записями см. раздел *Администрирование учетных записей пользователей и групп*.

Выход из системы или блокировка рабочей станции

Пользователь должен выходить из системы или блокировать рабочую станцию каждый раз, покидая рабочее место независимо от времени, в течение которого он собирается отсутствовать. Выход из системы позволяет другим пользователям зарегистрироваться в ней (если у них имеется учетная запись и они знают пароль); блокировка — не позволяет. Блокировку рабочей станции можно сделать автоматической при наличии любой 32-битной программы сохранения экрана.

Пароли

Любой, кто знает имя пользователя и связанный с ним пароль, может войти в систему. Поэтому храните пароли в секрете, а также:

- часто меняйте пароли;
- не используйте легко угадываемые слова или слова из словаря. Фразы или комбинации букв и цифр надежнее всего;
- не записывайте пароли. Выбирайте такой, чтобы Вам его было проще запомнить.

Защита файлов и каталогов

Файловая система NTFS обладает более развитыми свойствами защиты, чем FAT; поэтому ее необходимо использовать всегда, когда требуется защита. FAT применяется только на загрузочных разделах в ARC-совместимых RISC-системах. Системный раздел FAT можно защитить командой ***Secure System Partition*** из меню ***Partition*** в администраторе дисков ***Disk Administrator***.

Подробнее о защите и разграничении доступа на разделах NTFS см. главу *Файловая система NTFS*.

На практике убедитесь, что пользователи знают о том, что файл, перемещаемый или копируемый в другой каталог в пределах одного тома, имеет все атрибуты защиты, имевшиеся у него до копирования. Если, например, новый каталог не защищен, а является совместно используемым, переместите файл в другой, защищенный каталог, либо сразу при копировании наложите ограничения на доступ к нему.

Резервное копирование

Регулярное резервное копирование защитит Ваши данные от сбоев техники или ошибок, а также от вирусов и других повреждений. Подробнее см. раздел *Резервное копирование на магнитную ленту*.

Очевидно, для выполнения резервного копирования файлы должны быть прочитаны, а для восстановления — записаны. Привилегию резервного копирования должны иметь только члены групп **Administrators** и **Backup operators** — люди, которым Вы доверяете.

Защита реестра

Вся информация о конфигурации Windows NT хранится в реестре. Как правило, модификация ключей реестра выполняется специальными программами, например, через панель управления. Этот способ рекомендуется. Однако ключи можно изменять и в редакторе реестра, а некоторые из ключей — только в нем.

Работать с редактором реестра должен лишь тот, кто отлично понимает устройство реестра и работу с его редактором, а также представляет эффекты, вызываемые тем или иным параметром. Любое непрофессиональное изменение реестра может сделать систему неработоспособной. Подробнее см. главу *Использование реестра*.

Аудит

Аудит может проинформировать о действиях, повышающих риск нарушения защиты системы, и о пользователях, выполняющих эти действия. Подробнее см. главу *Аудит и мониторинг системы*.

Замечу: аудит только сообщает, какие бюжеты пользователей были задействованы при выполнении зафиксированных событий. Если пароли защищены соответствующим образом, это укажет пользователей, совершавших события. Но если пароль был украден или действия были совершены тогда, когда пользователь был зарегистрирован в системе, но отсутствовал на рабочем месте, это указывает на то, что события были совершены кем-то другим.

Определяя политику аудита, прикиньте, во что Вам обойдется (в терминах дискового пространства и загрузки процессора) аудит тех или иных событий в сравнении с важностью этих событий. Необходимо регистрировать по крайней мере попытки неудачных регистраций в системе, попытки доступа к важным данным и изменения параметров защиты. Ниже приведены наиболее общие случаи нарушения защиты и типы аудита, позволяющие их отслеживать.

<i>Нарушение защиты</i>	<i>Действие</i>
Использование произвольных паролей для подбора	Регистрация неудачных попыток регистрации в системе и выхода из нее.
Использование украденного пароля	Регистрация удачных попыток регистрации в системе и выхода из нее. В журнале регистрации при этом не будет видно никакой разницы между действиями "законного" пользователя и нарушителя. Однако анализируя, скажем, необычную активность в те дни, когда ее не должно быть, можно сделать вывод о незаконном использовании бюджета.
Неверное использование административных привилегий авторизованными пользователями	Регистрация удачного применения прав пользователей; управления пользователями и группами, изменений политики защиты; перезагрузок, выключений и системных событий. (Заметьте: в силу большого числа событий аудита WindowsNT обычно не регистрирует использование привилегий Backup Files And Directories и Restore Files And Directories .)
Вирусная атака	Регистрация удачных и неудачных попыток доступа к программным файлам с расширениями .EXE и .DLL. Регистрация удачного и неудачного отслеживания процессов. Запустите подозрительную программу и посмотрите в журнале попытки модификации программных файлов и создание неожиданных процессов. Помните: эта опция вызывает огромное число записей в журнале. Ее стоит использовать, только если Вы занимаетесь активным мониторингом системного журнала.
Неверный доступ к важным файлам	Регистрация удачных и неудачных попыток доступа к определенным файлам и объектам со стороны подозрительных пользователей и групп.
Неверный доступ к принтерам	Регистрация удачных и неудачных попыток доступа к файлам и объектам и, в частности, к принтерам со стороны подозрительных пользователей и групп.

Управление журналом безопасности

Можно указать максимальный размер файла регистрации и события, которые произойдут при его переполнении. Подробно см. главу *Аудит и мониторинг системы*.

Одна из задач администратора сети — регулярная проверка журнала защиты для отслеживания важных записей и мониторинга использования системы, а также очистка журнала по мере необходимости. Рекомендуется регулярно архивировать содержимое журнала перед его очисткой.

Дополнительно рекомендуется не пренебрегать советами, приведенными в главе 2 "Windows NT Security Model" в *Windows NT Resource Guide*.

Установки, обеспечивающие высокую степень защиты

Стандартных средств защиты обычно достаточно. Однако в ряде случаев имеет смысл применять дополнительные меры.

Требования физической защиты

Требования физической защиты, рассматривавшиеся для минимальной и обычной степеней защиты, применимы и в данном случае. Дополнительно следует обратить внимание на физическое подключение компьютера к сети, а в некоторых случаях применять специальные встроенные устройства, позволяющие физически ограничить доступ к выключателю питания.

Сети и безопасность

Подключая компьютер к сети, Вы тем самым предоставляете путь в свой компьютер. Желание обезопасить этот путь вполне естественно. Регистрации пользователей и защиты файлов и других объектов достаточно для обеспечения стандартного уровня защиты, однако для высокой степени защиты необходимо убедиться в защищенности самой сети или даже полностью изолировать компьютер от сети.

В сетевых подключениях опасность могут представлять другие пользователи или неавторизованные подключения. Если все в сети имеет средства защиты для доступа к Вашему защищенному компьютеру, то скорее всего Вы подключите компьютер к сети для облегчения доступа к Вашему компьютеру.

Когда сеть целиком расположена в охраняемом помещении, риск неавторизованных подключений минимизирован или просто исключен. Если же проводка местами проходит через неохраняемые участки, используйте на них оптоволоконные линии, исключающие возможность ответвления.

Чтобы доступ в Internet также был безопасен, воспользуйтесь рекомендациями, приведенными в главе *Построение глобальных сетей и работа с Internet*.

Контроль за доступом к выключателю питания

Необходимо следить за тем, чтобы неавторизованные пользователи не имели доступа к выключателю питания или кнопке “Сброс” компьютера, особенно когда политика защиты в Вашей организации запрещает им выполнять выключение компьютера. У самых защищенных компьютеров (кроме тех, что разме-

щаются в закрытых и охраняемых помещениях) открыта только клавиатура, монитор, мышь и (когда надо) принтер. ЦПУ и съемные накопители должны быть заперты и доступны лишь для специального персонала.

Многие аппаратные платформы могут быть защищены *паролем включения*. Он препятствует неавторизованному персоналу загрузить на компьютере систему, отличную от Windows NT. Пароль включения — функция аппаратуры, а не операционной системы. Поэтому установка такого пароля зависит от типа компьютера и выполняется в соответствии с указаниями, приведенными в документации на компьютер.

Требования программной защиты

Некоторые параметры повышенной защищенности можно реализовать только с помощью редактора реестра. Право работать с редактором реестра получают администраторы, подробно ознакомившиеся с частью IV "Windows NT Registry" в *Windows NT Resource Guide*.

Привилегии пользователей

Ряд привилегий в системах с высокой степенью защиты является объектом постоянного внимания и аудита со стороны администраторов. Советую изменить описанные ниже привилегии с установленных по умолчанию на рекомендуемые:

<i>Привилегия</i>	<i>Группы, обладающие по умолчанию</i>	<i>Рекомендуемое изменение</i>
Log on locally Позволяет пользователю регистрироваться локально, с клавиатуры компьютера.	Administrators, Backup Operators, Everyone, Guests, Power Users, Users	Запретить группам Everyone и Guests .
Shut down the system Позволяет пользователям выключать Windows NT.	Administrators, Backup Operators, Everyone, Power Users, Users	Запретить Everyone и Users .

Привилегии, перечисленные в таблице ниже, вообще-то не требуют каких-либо изменений относительно значений, установленных по умолчанию.

<i>Привилегия</i>	<i>Позволяет</i>	<i>Изначально назначается</i>
Access this computer from the network	Пользователю подключаться к компьютеру по сети.	Administrators, Everyone, Power Users
Act as part of the operating system	Действовать, как защищенная и надежная часть операционной системы.	(Никому)

<i>Привилегия</i>	<i>Позволяет</i>	<i>Изначально назначается</i>
Add workstations to the domain	Данная привилегия не имеет никакого эффекта на машинах, работающих под Windows NT.	(Никому)
Back up files and directories	Пользователю выполнять резервное копирование файлов и каталогов. Эта привилегия имеет превосходство над правами доступа к файлам и каталогам.	Administrators, Backup Operators
Bypass traverse checking	Пользователю изменять каталоги и осуществлять доступ к файлам в подкаталогах, даже если доступ к родительскому каталогу закрыт.	Everyone
Change the system time	Пользователю устанавливать внутренний таймер компьютера.	Administrators, Power Users
Create a pagefile	Данная привилегия не имеет никакого эффекта на машинах, работающих под Windows NT.	Administrators
Create a token object	Процессам создавать маркеры доступа.	(Никому)
Create permanent shared objects	Пользователю создавать специальные постоянные объекты типа \\Device, которые используются в Windows NT.	(Никому)
Debug programs	Пользователю отлаживать различные низкоуровневые объекты типа потоков.	Administrators
Force shutdown from a remote system	Данная привилегия не имеет никакого эффекта на машинах, работающих под Windows NT.	Administrators, Power Users
Generate security audits	Процессу создавать записи в журнале аудита защиты.	(Никому)
Increase quotas	Данная привилегия не имеет никакого эффекта на машинах, работающих под Windows NT.	(Никому)

<i>Привилегия</i>	<i>Позволяет</i>	<i>Изначально назначается</i>
Increase scheduling priority	Пользователю увеличивать приоритет процесса.	Administrators, Power Users
Load and unload device drivers устройств	Пользователю устанавливать и удалять драйверы.	Administrators
Lock pages in memory	Пользователю записывать страницы в памяти, так что они не могут быть сброшены в PAGEFILE.SYS.	(Никому)
Log on as a batch job	Данная привилегия не имеет никакого эффекта на машинах, работающих под Windows NT.	(Никому)
Log on as a service	Процессу регистрироваться в системе как сервис.	(Никому)
Manage auditing and security log	Пользователю указывать, какие типы доступа к ресурсам подлежат регистрации, а также просматривать и очищать журнал аудита.	Administrators
Modify firmware environment variables	Пользователю изменять переменные системного окружения, хранящиеся в долговременной памяти систем, поддерживающих такой тип конфигурирования.	Administrators
Profile single process	Пользователю выполнять профилирование процесса.	Administrators, Power Users
Profile system performance	Пользователю выполнять профилирование системы.	Administrators
Replace a process-level token	Пользователю изменять маркер контроля доступа к процессу.	(Никому)
Restore files and directories	Пользователю восстанавливать зарезервированные файлы и каталоги.	Administrators, Backup Operators
Take ownership of files or other objects	Пользователю вступать во владение файлами, каталогами, принтерами и другими объектами.	Administrators

Защита файлов и каталогов

В число файлов и каталогов, подлежащих защите, входят файлы, принадлежащие самой операционной системе. Стандартный набор прав доступа к системным файлам и каталогам обеспечивает разумную степень защиты. Однако для систем с высокой степенью защиты имеет смысл сразу после установки системы предоставить права доступа к файлам и каталогам в соответствии с таблицей, приведенной ниже. Не забудьте, что сначала надо предоставлять доступ к родительским каталогам, а потом — к вложенным.

<i>Каталог</i>	<i>Права доступа</i>
\WINNT35	Administrators: Full Control CREATOR OWNER: Full Control Control Everyone: Read SYSTEM: Full Control
\WINNT35\REPAIR	Administrators: Full Control
\WINNT35\SYSTEM	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\SYSTEM32	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\SYSTEM32\CONFIG	Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control
\WINNT35\SYSTEM32\DHCP	(Удалить)
\WINNT35\SYSTEM32\DRIVERS	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\SYSTEM32\RAS	(Удалить)
\WINNT35\SYSTEM32\OS2	(Удалить)
\WINNT35\SYSTEM32\SPOOL	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control
\WINNT35\SYSTEM32\WINS	(Удалить)

Некоторые критичные для работы операционной системы файлы находятся в корневом каталоге системного раздела диска компьютеров с процессорами Intel® 80486 и Pentium®. В системах с высокой степенью защиты установите следующие права доступа к этим файлам.

<i>File</i>	<i>C2-Level Permissions</i>
\BOOT.INI, \NTDETECT.COM, \NTLDR	Administrators: Full Control SYSTEM: Full Control
\AUTOEXEC.BAT, \CONFIG.SYS	Everybody: Read Administrators: Full Control SYSTEM: Full Control

Для просмотра этих файлов в **File Manager** выберите в меню **View** команду **By File Type** и пометьте флажок **Show Hidden/System Files**.

Защита реестра

В дополнение к требованиям стандартной защиты администратор систем с высокой защитой должен установить защиту некоторых ключей в реестре.

По умолчанию различные компоненты реестра защищены таким образом, чтобы обеспечивать стандартный уровень безопасности. Для обеспечения высокого уровня безопасности надо указать права доступа к определенным ключам реестра. Делать это следует чрезвычайно внимательно, так как программы, выполняемые пользователями, часто нуждаются в доступе к различным ключам "от имени" пользователя.

В частности, для следующих ключей группа **Everyone** должна иметь только права **QueryValue**, **Enumerate Subkeys**, **Notify**, и **Read**.

В диалоговом окне HKEY_LOCAL_MACHINE on Local Machine:

```

\Software\Microsoft\RPC (и все подключки)
\Software\Microsoft\WindowsNT\CurrentVersion
В поддепеve \Software\Microsoft\WindowsNT\CurrentVersion\
  Profile List
  AeDebug
  Compatibility
  Drivers
  Embedding
  Fonts
  FontSubstitutes
  GRE_Initialize
  MCI
  FontSubstitutes
  GRE_Initialize
  MCI
  MCI Extensions
  Port (и все подключки)
  WOW (и все подключки)
  Windows3.1MigrationStatus (и все подключки).
```

В диалоговом окне HKEY_CLASSES_ROOT on Local Machine:

HKEY_CLASSES_ROOT (и все подключки).

Сервис планирования (команда AT)

Сервис планирования (известный по команде **AT**) используется для автоматического запуска заданий в установленное время. Так как запланированное задание выполняется в контексте планировщика (обычно контекст операционной системы), то в системах с высокой степенью защиты планировщик использовать нельзя.

По умолчанию только администраторы могут выполнять команды **AT**. Чтобы системные операторы тоже могли применять команду **AT**, используйте редактор реестра для создания следующего значения:

Улей:	HKEY_LOCAL_MACHINE\SYSTEM
Ключ:	\CurrentControlSet\Control\Lsa
Имя:	Submit Control
Тип:	REG_DWORD
Значение:	1

Предоставить право исполнения команды **AT** еще кому-либо невозможно. Изменения вступят в силу после перезагрузки компьютера. Также желательно обновить **Emergency Repair Disk** для отражения внесенных изменений.

Соккрытие имени последнего пользователя

По умолчанию в Windows NT имя последнего зарегистрировавшегося на компьютере пользователя помещается в поле **Username** диалогового окна регистрации. Это сделано для удобства пользователя, обычно регистрирующегося на данном компьютере. Для содействия сохранению имен пользователей в секрете в Windows NT можно запретить отображение имени последнего зарегистрировавшегося пользователя. Это особенно важно, если через общедоступный компьютер осуществлялся доступ с измененным именем администратора.

Чтобы запретить показ имени пользователя в диалоговом окне регистрации, используйте редактор реестра для создания или переопределения следующего ключа:

Улей:	HKEY_LOCAL_MACHINE\SOFTWARE
Ключ:	\Microsoft\WindowsNT\Current Version\Winlogon
Имя:	DontDisplayLastUserName
Тип:	REG_SZ
Значение:	1

Ограничение процесса загрузки

На большинстве современных ПК поддерживается возможность загрузки различных операционных систем. Например, если Вы обычно загружаете Windows NT с диска C., кто-либо может выбрать иную версию Windows на другом диске, включая гибкий или CD-ROM-диск. Если это произойдет, все меры безопасности, предпринятые Вами в обычной версии Windows NT, могут быть нарушены.

Вообще на компьютере необходимо устанавливать только те операционные системы, которые Вы хотите использовать. Для систем с высокой степенью защиты это означает установку только одной версии Windows NT. Однако процессор необходимо защитить физически, чтобы никто другой не смог установить иную операционную систему. В зависимости от обстоятельств можно исключить накопители на гибких дисках. В некоторых компьютерах можно запретить загрузку с гибких дисков путем установки перемычек или переключателей внутри процессорного блока. При этом либо закройте корпус компьютера (если это возможно), либо поставьте компьютер в отдельном защищенном помещении.

Разрешение выключать компьютер только зарегистрированным пользователям

Обычно для выключения Windows NT Workstation без регистрации в системе надо щелкнуть кнопку **Shutdown** в диалоговом окне регистрации. Выполнение shutdown необходимо, если пользователи имеют доступ к выключателю питания или кнопке Reset; в противном случае они могут ими воспользоваться, что приведет к ненормальному выключению системы. Если же пользователи лишены доступа к столь ответственным кнопкам, можно запретить выполнять shutdown без регистрации в системе. Этот шаг не требуется для Windows NT Server, так как он сконфигурирован для этого по умолчанию.

Чтобы пользователи могли заглушить систему только после предварительной регистрации в ней, внесите в реестр следующие изменения и перезагрузите компьютер:

Улей:	HKEY_LOCAL_MACHINE\SOFTWARE
Ключ:	\Microsoft\WindowsNT\Current Version\Winlogon
Имя:	ShutdownWithoutLogon
Тип:	REG_SZ
Значение:	0

Желательно обновить **Emergency Repair Disk** для отражения внесенных изменений.

Контроль за доступом к съемным устройствам хранения

По умолчанию Windows NT позволяет любой программе осуществлять доступ к файлам на гибких или компакт-дисках. В системах с высокой степенью защиты и в многопользовательских условиях рекомендуется предоставлять доступ к таким устройствам только тем, кто непосредственно работает за компьютером. Это позволит заносить информацию на такие носители, не опасаясь, что другой пользователь или программа модифицируют эти данные.

При работе в таком режиме накопители на гибких или компакт-дисках предоставляются пользователю в процессе регистрации. При выходе пользователя из системы к этим устройствам предоставляется свободный доступ. Поэтому важно всю информацию, хранящуюся на них, удалить до выхода из системы.



Примечание: В Windows NT любой пользователь имеет доступ к накопителю на магнитной ленте и, таким образом, может записать и прочитать содержимое ленты. Вообще это не опасно, так как интерактивно работать на компьютере может только один пользователь. Но существует небольшая вероятность того, что программа, запущенная предыдущим пользователем, продолжает выполняться даже после его выхода из системы. Когда следующий пользователь поместит ленту в накопитель, программа скрытно передаст важную информацию с ленты. Во избежание этого перезагрузите компьютер перед использованием ленты.

Предоставление гибких дисков при регистрации

Используйте редактор реестра для модификации или создания следующего ключа:

Улей:	HKEY_LOCAL_MACHINE\SOFTWARE
Ключ:	\Microsoft\WindowsNT\CurrentVersion\Winlogon
Имя:	AllocateFloppies
Тип:	REG_DWORD
Значение:	1

Если этого ключа нет или установлено иное значение, гибкие диски будут доступны для совместного использования всеми процессами системы.

Это значение сработает только при следующей регистрации и не окажет никакого эффекта в течение текущего сеанса. Пользователь должен выйти из системы и зарегистрироваться вновь.

Предоставление компакт-дисков при регистрации

Используйте редактор реестра для создания или модификации следующего ключа:

Улей:	HKEY_LOCAL_MACHINE\SOFTWARE
Ключ:	\Microsoft\WindowsNT\CurrentVersion\Winlogon
Имя:	AllocateCDRoms
Тип:	REG_DWORD
Значение:	1

Если этого ключа нет или установлено иное значение, компакт-диски будут доступны для совместного использования всеми процессами системы.

Это значение сработает только при следующей регистрации и не окажет никакого эффекта в течение текущего сеанса. Пользователь должен выйти из системы и зарегистрироваться вновь.

Установки, необходимые для соответствия защиты уровню C2

В этом приложении описаны конфигурация и настройка системы, использовавшиеся при сертификации Windows NT на соответствие уровню C2. Во многом эти требования повторяют описанные в приложении В, однако в данном случае они привязаны к определенной технике. Аппаратные платформы, использовавшиеся при этом, перечислены в Приложении Д. Все сказанное ниже относится к Windows NT Workstation и Windows NT Server версии 3.5.

- Распакуйте и установите технику.

Следуйте инструкции, прилагаемой к технике.

- Установите ARC-соответствующее firmware.

Если Ваша RISC-система не сконфигурирована на использование ARC-соответствующего firmware, установите его отдельно в соответствии с прилагаемыми к нему инструкциями. Свяжитесь с представителями Digital Equipment Corporation (DEC™) или поставщиком Вашей техники для получения текущей версии ARC-соответствующего firmware. В системах Alpha AXP™/150 должно быть firmware версии 3.5-5 для соответствия уровню защиты C2.

- Установите пароль включения.

Для этого:

На компьютерах фирмы Compaq® Computer Corporation

1. Вставьте компакт-диск SmartStart® в накопитель на CD и включите питание компьютера. Компьютер загрузится с компакт-диска и запустит утилиту **SmartStart**.
2. Выберите в меню **Non-SmartStart Setup**.
3. Выберите **System Configuration** в меню **Manual Configuration And Server Utilities**.
4. Выберите **Configure Hardware** в меню **System Configuration**. Утилита попытается сконфигурировать технику автоматически, а затем появится диалоговое окно **Configuration Complete**.
5. Выберите **Review Or Modify Hardware Settings** и нажмите клавишу Enter.
6. В меню **Steps In Configuring Your Computer** выберите **Step 3: View Or Edit Details**, а затем нажмите клавишу Enter.

7. В диалоговом окне **View Or Edit Details** выберите **Set Power-On Password: Disabled**.
8. Введите пароль и нажмите клавишу Enter. Затем введите пароль снова и нажмите Enter.
9. Нажмите клавишу F10.
10. В меню **Steps In Configuring Your Computer** выберите **Step 5: Save And Exit**, а затем нажмите клавишу Enter.
11. Нажмите клавишу Enter.
12. В меню **Save and Edit** выберите **Save the Configuration and Restart** и нажмите клавишу Enter.



ВНИМАНИЕ: Существует возможность того, что нарушитель откроет компьютер и получит доступ к переключателям, запрещающим использование пароля включения. Кроме того, он может установить дополнительный жесткий диск с менее защищенной операционной системой или с Windows NT, но не включающей установок защиты. Поэтому необходимо принять меры для предотвращения такого доступа. Если модель компьютера позволяет, его надо запечатать, либо поставьте компьютер в защищенном, хорошо вентилируемом помещении.

На компьютерах с процессором Alpha AXP фирмы Digital Equipment Corporation:

1. Включите компьютер.
2. В меню **Boot** выберите **Supplementary**.
3. В меню **Supplementary** выберите **Set Up The System**.
4. В меню **Setup** выберите **Set Firmware Password**.
5. Введите пароль дважды, а затем нажмите клавишу Enter.
6. Нажмите клавишу Esc для выхода в меню **Supplementary**.

Процесс установки пароля завершен.

► Установите Windows NT.

Установку Windows NT выполняйте в соответствии с инструкциями, приведенными в главе 1 "Installing Windows NT Workstation" в руководстве *Windows NT Workstation Installation Guide*. При этом:

1. Вы должны выбрать настраиваемую установку (**Custom Setup**). Это позволит установить только необходимые компоненты.
2. Все разделы жесткого диска должны быть отформатированы в NTFS, кроме небольшого системного раздела (2-MB) для RISC-систем. Подробнее о разбиении диска на разделы см. раздел "Speci-

fyng the Disk Partitions” в главе 1 “Installing Windows NT Workstation” руководства *Windows NT Workstation Installation Guide*. Для соответствия уровню защиты C2 на компьютере не должно быть установлено никаких других операционных систем.

3. Вы не должны устанавливать сетевое программное обеспечение. Если Вы устанавливаете Windows NT Server, в диалоговом окне **Windows NT Server Security Role** выберите опцию **Server**. При установке как Windows NT Workstation, так и Windows NT Server при появлении текста “Setup will perform the following optional tasks...” сбросьте флажок **Set Up Network**.
 4. В диалоговом окне **Administrator Account Setup** не оставляйте административный пароль пустым. Длина введенного пароля должна составлять минимум 6 символов, отгадать которые было бы непросто.
 5. В диалоговом окне **Local Account** можно создать учетную запись для пользователя, выполняющего на компьютере обычную работу. Помните: по умолчанию эта учетная запись будет включена в административную группу, позволяющую создавать новые учетные записи. Подробнее о возможностях группы **Administrators** см. раздел *Привилегии встроенных учетных записей в этой книге*.
 6. Создайте **Emergency Repair Disk**. Это поможет облегчить восстановление системы, если база данных конфигурации будет повреждена.
- Запустите WindowsNT и зарегистрируйтесь как **Administrator**.
- Перезагрузите компьютер и запустите Windows NT. Зарегистрируйтесь под административной учетной записью **Administrator**. Она позволит выполнить остальные шаги по конфигурированию.
- Установите Microsoft Windows NT 3.5 Workstation и Server U.S. Service Pack 3.
1. Если установка Service Pack выполняется с гибких дисков, вставьте диск 1 в соответствующее устройство. При установке с компакт-диска вставьте диск в накопитель CD-ROM.
 2. В **Program Manager** выберите команду **Run** в меню **File**.
 3. Для запуска программы установки введите **диск:\система\update** [где *система* соответствует типу компьютера (например **Alpha** или **i386™**), а диск — буква, соответствующая диску, содержащему установочную дискету или компакт-диск]. Далее следуйте инструкциям программы.
- Запретите работу подсистем OS/2® и POSIX.

Для запрета подсистем OS/2 и POSIX используйте редактор реестра, как это описано в *Windows NT Resource Guide*, для удаления любого текста, связанного с ключом реестра:

Улей:	HKEY_LOCAL_MACHINE\SYSTEM
Ключ:	CurrentControlSet\Control\Session Manager\ SubSystems
Имя:	Произвольное
Значение:	Null

Изменения вступят в силу после перезагрузки системы. Вы можете обновить **Emergency Repair Disk** для отражения внесенных изменений.

- Защитите системный раздел (только на RISC-системах).

На RISC-компьютере запустите **Disk Administrator** и выберите команду Secure System Partition в меню Partition. Это обеспечит возможность доступа к файлам на системном разделе только пользователям, принадлежащим к группе администраторов.

- Измените значок **User Manager**.

Если Вы устанавливаете Windows NT Server, удалите программный элемент **User Manager For Domains** и добавьте **User Manager**, как это описано в главе "Program Manager" в *Windows NT Server System Guide*. Имя исполняемого файла, соответствующего **User Manager**, — MUSRMGREXE.

- Установите минимальную длину пароля (см. раздел *Изменение минимальной длины пароля*).
- Запретите использование учетной записи **Guest** (см. раздел *Учетная запись Guest*).
- Ограничьте использование привилегий и прав пользователей (см. раздел *Изменение привилегий пользователей*). Привилегии должны быть ограничены в соответствии со следующей таблицей:

<i>Привилегия</i>	<i>Дана по умолчанию</i>	<i>Для соответствия уровню C2</i>
Access this computer from the network	Administrators, Everyone, Power Users	Не требуется изменений.
Act as part of the operating system	(Никому)	Не требуется изменений; не давать никому.
Add workstations to the domain	(Никому)	Не требуется изменений.
Back up files and directories	Administrators, Backup Operators	Не требуется изменений.
Bypass traverse checking	Everyone	Не требуется изменений.
Change the system time	Administrators, Power Users	Не требуется изменений.
Create a pagefile	Administrators	Не требуется изменений.
Create a token object	(Никому)	Не требуется изменений; не давать никому.

<i>Привилегия</i>	<i>Дана по умолчанию</i>	<i>Для соответствия уровню C2</i>
Create permanent shared objects	(Никому)	Не требуется изменений.
Debug programs	Administrators	Удалить Administrators . Эта привилегия не подлежит аудиту, поэтому ее нельзя предоставлять кому бы то ни было, включая администраторов.
Force shutdown from a remote system	Administrators, Power Users	Не требуется изменений.
Generate security audits	(Никому)	Не требуется изменений; не давать никому.
Increase quotas	(Никому)	Не требуется изменений.
Increase scheduling priority	Administrators, Power Users	Не требуется изменений.
Load and unload device drivers	Administrators	Не требуется изменений.
Lock pages in memory	(Никому)	Не требуется изменений.
Log on as a batch job	(Никому)	Не требуется изменений.
Log on as a service	(Никому)	Не требуется изменений.
Log on locally	Administrators, Backup Operators, Guests, Power Users, Users	Удалить группу Guests .
Manage auditing and security log	Administrators	Не требуется изменений.
Modify firmware environment variables	Administrators	Не требуется изменений.
Profile single process	Administrators, Power Users	Не требуется изменений.
Profile system performance	Administrators	Не требуется изменений.
Replace a process-level token	(Никому)	Не требуется изменений; не давать никому.
Restore files and directories	Administrators, Backup Operators	Не требуется изменений.
Shut down the system	Administrators, Backup Operators, Power Users, Users	Удалить группу Users .
Take ownership of files or other objects	Administrators	Не требуется изменений.

- Разрешить выключение системы только зарегистрированными пользователями.

Установив Windows NT Workstation, убедитесь, что компьютер нельзя выключить без предварительной регистрации. Этот шаг можно пропустить, если Вы установили Windows NT Server, так как для него это устанавливается по умолчанию.

Для разрешения выключения компьютера только зарегистрированными пользователями используйте редактор реестра для редактирования значения ключа:

Улей:	HKEY_LOCAL_MACHINE\SOFTWARE
Ключ:	\Microsoft\WindowsNT\Current Version\Winlogon
Имя:	ShutdownWithoutLogon
Значение:	0

- Установите поведение журнала безопасности.

Используйте **Event Viewer** для установки параметров журнала безопасности. Выберите опцию **Do Not Overwrite Events (Clear Log Manually)**. Дополнительно можно предписать Windows NT останавливаться в случае невозможности аудита события так, как это описано в главе *Аудит и мониторинг системы*. Можно указать на необходимость регистрации применения привилегий, с помощью редактора реестра создав или модифицировав следующие значения:

Улей:	HKEY_LOCAL_MACHINE
Ключ:	SYSTEM\CurrentControlSet\Control\Lsa
Имя:	FullPrivilegeAuditing
Тип:	REG_BINARY
Значение:	1

Изменения вступят в силу после следующей перезагрузки системы. Вы можете обновить **Emergency Repair Disk** для отражения внесенных изменений.

- Определите правила работы с гибкими дисками или компакт-дисками.

Для предоставления возможности использования гибких дисков или компакт-дисков только зарегистрированным пользователям в редакторе реестра создайте или измените следующие значения:

Улей:	HKEY_LOCAL_MACHINE\SOFTWARE
Ключ:	\Microsoft\WindowsNT\CurrentVersion\Winlogon
Имя:	AllocateFloppies
Тип:	REG_DWORD
Значение:	1

Улей:	HKEY_LOCAL_MACHINE\SOFTWARE
Ключ:	\Microsoft\WindowsNT\CurrentVersion\Winlogon
Имя:	AllocateCDRoms
Тип:	REG_DWORD
Значение:	1

Если значение не установлено или имеет другую величину, накопители на гибких дисках будут доступны для совместного использования всеми процессами системы.

Изменения вступят в силу после следующей регистрации в системе. Если пользователь уже зарегистрирован на момент установки значения, оно не будет активизировано до следующего сеанса работы. Пользователь должен разрегистрироваться, а затем зарегистрироваться вновь.

► **Защитите файлы и каталоги операционной системы.**

Используйте **File Manager** для установки прав доступа к каталогам и файлам, как это указано в таблице:

Каталог	Права доступа
\WINNT35	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\REPAIR	Administrators: Full Control
\WINNT35\SYSTEM	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\SYSTEM32	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\SYSTEM32\NTBACKUP.EXE	Administrators: Full Control SYSTEM: Full Control
\WINNT35\SYSTEM32\CONFIG	Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control
\WINNT35\SYSTEM32\DHCP	(Удалите этот каталог)
\WINNT35\SYSTEM32\DRIVERS	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control
\WINNT35\SYSTEM32\RAS	(Удалите этот каталог)
\WINNT35\SYSTEM32\OS2	(Удалите этот каталог)

<i>Каталог</i>	<i>Права доступа</i>
\WINNT35\SYSTEM32\SPOOL	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control
\WINNT35\SYSTEM32\WINS	(Удалите этот каталог)

Изменение прав доступа к \WINNT35\SYSTEM32\NTBACKUP.EXE делает невозможным пользователям выполнять резервное копирование. Если же Вы хотите, чтобы отдельные пользователи могли выполнять резервное копирование, создайте отдельный каталог для NTBACKUP.EXE и пользователям, которые будут делать резервное копирование, предоставьте полный доступ.

Некоторые критичные системные файлы располагаются в корневом каталоге системного раздела диска на системах Intel 80486 и Pentium. На эти файлы необходимо установить следующие права доступа:

<i>Файл</i>	<i>Права доступа для уровня C2</i>
\BOOT.INI, \NTDETECT.COM, \NTLDR	Administrators: Full Control SYSTEM: Full Control
\AUTOEXEC.BAT, \CONFIG.SYS	Everyone: Read Administrators: Full Control SYSTEM: Full Control

► Защитите ключи реестра.

Используйте редактор реестра для защиты перечисленных ниже ключей так, чтобы группа **Everyone** имела только следующие виды доступа: **QueryValue**, **Enumerate Subkeys**, **Notify** и **Read Control**.

В диалоговом окне HKEY_LOCAL_MACHINE on Local Machine:

\Software\Microsoft\RPC (и все подключки)

\Software\Microsoft\WindowsNT\CurrentVersion

Для \Software\Microsoft\WindowsNT\CurrentVersion\ все ветви:

Profile List

AeDebug

Compatibility

Drivers

Embedding

Fonts

FontSubstitutes

GRE_Initialize

MCI

MCI Extensions

MidiMap

Port (и все подключки)

WOW (и все подключки)

Windows3.1MigrationStatus (и все подключки).

В диалоговом окне HKEY_CLASSES_ROOT on Local Machine:

\HKEY_CLASSES_ROOT (и все подключи).

- Ограничьте управление буквами дисков и принтерами.

Управление буквами дисков и принтерами ограничивается в редакторе реестра созданием или указанием значений для ключей реестра:

Улей:	HKEY_LOCAL_MACHINE
Ключ:	SYSTEM\CurrentControlSet\Control\Session Manager
Имя:	ProtectionMode
Тип:	REG_DWORD
Значение:	1

- Перегрузите компьютер.
- Обновите ***Emergency Repair Disk***.

При потере системных файлов используйте ***Emergency Repair Disk***, а не утилиту ***Restore Backup*** и ***Restore*** не копируют системные списки контроля доступа (SACL). Восстанавливает эту информацию только ***Emergency Repair Disk***.

Системы, на которых Windows NT сертифицирован на соответствие уровню C2

При проверке Windows NT на соответствие уровню защиты C2 использовались следующие компьютеры:

Compaq[®] ProLiant[™] 2000 и 4000

DECpc AXP/150

Compaq ProLiant 2000 и 4000

Компьютеры фирмы Compaq моделей ProLiant 2000 и ProLiant 4000 использовались при тестировании Windows NT на соответствие уровню защиты C2. ProLiant 2000 поддерживает до 2 процессоров, а ProLiant 4000 — до 4 процессоров. Они предназначены для использования в качестве файл-серверов, однако рассматривались как отдельно стоящие компьютеры с отключенными сетевыми возможностями. При тестировании рассматривались следующие компоненты:

<i>Компонент</i>	<i>Описание</i>	<i>Производитель</i>	<i>Номер по каталогу Compaq</i>
Системная плата	Tri-Flex EISA	Compaq	Tri-Flex
Процессорный модуль	Pentium/90	Compaq	199050-001
	Pentium/100	Compaq	163888-001
Память	16 MB, 70 ns	Compaq	149949-001
	32 MB, 70 ns	Compaq	149912-001
	64 MB, 70 ns	Compaq	149913-001
	128 MB, 70 ns	Compaq	149914-001
Видеоадаптер	SVGA 1024x768x4	Compaq	(На плате)
SCSI-контроллер	32-bit FAST SCSI-2	Compaq	142013-001
НЖМД	1.5 GB SCSI-2	Compaq	146742-003
	2.1 GB SCSI-2	Compaq	146742-004
Съемные диски	CD-ROM	Compaq	142193-001
	3.5" 1.44 MB FDD	Compaq	113638-001
	4.0 GB DAT	Digital	TLZ07
	2/8 GB DAT	Compaq	142019-001
Клавиатура	101-key English	Compaq	160650-101
Мышь	3-button	Compaq	141649-002
Принтер	HP [®] LaserJet [®] IV	Hewlett-Packard [®]	

Проверка целостности процессора

Производитель компьютера поставяет совместно с ним диагностические тесты, позволяющие контролировать правильность работы компьютера. Необходимо выполнить такую проверку перед установкой Windows NT, а затем выполнять ее на регулярной основе. В документации, поставляемой с компьютером, приведены инструкции по проведению этих тестов и расшифровка результатов. В дополнение к диагностике, поставляемой производителями компьютеров на базе процессоров Intel 80486 и Pentium, существует диагностический тест процессоров этих компьютеров. Этот тест можно получить, позвонив в лабораторию Lone Star Evaluation Laboratories по телефону 1-800-535-5735 или (512)746-2251.

Проверка целостности периферии

Для проверки правильности работы периферийных устройств совместно с описанными в данном приложении компьютерами используйте тесты, поставляемые вместе с компьютерами.

DECpc AXP/150

Система фирмы DEC, участвовавшая в тестировании Windows NT на соответствие уровню защиты C2, DECpc AXP/150 может быть сконфигурирована для работы в качестве сервера или рабочей станции. Она тестировалась с отключенными сетевыми возможностями. В таблице перечислены компоненты, включенные в тестирование.

<i>Компонент</i>	<i>Описание</i>	<i>Производитель</i>	<i>Номер по каталогу Digital</i>
Системная плата	EISA	Digital	PB22H-KB
Процессор	21064-AA/150	Digital	54-20674-04
Видеоадаптер	Qvision® SVGA	Compaq	PB2GA-AA
SCSI-контроллер	Adaptec™ 1742	Adaptec	PB2HA-SA
	High Performance	Adaptec	PCTAZ-AB
	Low Cost	Adaptec	PCTAZ-AD
НЖМД	535 MB SCSI	Digital	PB2RA-EA
	126 MB SCSI	Digital	RZ25
	1.6 GB SCSI	Digital	RZ27
	2.0 GB SCSI	Digital	RZ28
Съемные диски	CD-ROM RRD42	Digital	PB2SA-AA
	3.5" 1.44 MBFDD	Digital	RX26-AA
	525 MB QIC Tape	Digital	TZK10
	4.0 GB DAT	Digital	TLZ07
	395 MB Cartridge Tape	Digital	TZ30

<i>Компонент</i>	<i>Описание</i>	<i>Производитель</i>	<i>Номер по каталогу Digital</i>
Клавиатура	101-key English	Digital	PCXAL-FA
Мышь	3-button	Digital	PCXAS-AA
Принтер	HP LaserJet IV	Hewlett-Packard	

Проверка целостности процессора

Тесты целостности процессора для конфигурации, описанной в этом приложении, можно найти в каталоге ALPHASYS на компакт-диске Service Pack 3. В файле README.TXT содержатся указания по запуску этих тестов.

Проверка целостности периферии

Hardware Compatibility Test (HCT), распространяемый Microsoft на диске MSDN level 2, использовался при тестировании на соответствие уровню C2 целостности периферийных устройств. Для приобретения MSDN level 2 обращайтесь к партнерам Microsoft.

А

Авторизация

Проверка регистрационной информации о пользователе. Если пользователь регистрируется на *Windows NT Workstation*, авторизация выполняется на этой *рабочей станции*. При регистрации пользователя в *домене* авторизация выполняется на *контроллере домена*. См. *Доверительные отношения*.

Административные сигналы тревоги

Когда в компьютере генерируется административный сигнал тревоги, предустановленному списку пользователей или компьютеров рассылаются сообщения. Эти сообщения относятся к *серверу* и *ресурсам*. Они предупреждают о нарушении защиты и доступа, проблемах сеансов пользователей, выключениях сервера при сбоях питания (при наличии *UPS*), проблемах тиражирования *каталогов*, проблемах печати. Занимается этим *сервис Alerter*.

Аудит

Проверка элементов управления системой.

Аудит каталогов

Отслеживание использования одного или нескольких *каталогов*.

Аудит печати

Функция, позволяющая отслеживать доступ к определенным принтерам.

Аудит приложений

Регистрация событий, связанных с процессами ввода, обработки и вывода внутри приложений.

Аудит реестра

Отслеживание событий, связанных с попытками открыть *ключ реестра* или извлечь из него информацию.

Аудит страницы Книги обмена

Функция, позволяющая отслеживать работу отдельных пользователей с содержимым *страницы Книги обмена*.

Аудит удаленного доступа

Функция, позволяющая отслеживать деятельность *серверов* удаленного доступа.

Аудит файлов

Отслеживание использования одного или нескольких файлов

Аутентификация

См. Авторизация.

Б

База данных домена

См. База данных SAM.

База данных SAM

База данных информации безопасности, содержащая имена *учетных записей пользователей* и *пароли*, а также установки политики безопасности. В *Windows NT Workstation* управление базой SAM выполняется в *User Manager*, а в *Windows NT Server* — в *User Manager for Domains*.

Блокировка учетной записи

Функция, позволяющая блокировать определенную *учетную запись* на заданный промежуток времени при превышении указанного количества неудачных попыток регистрации в системе.

Буфер

Место для временного хранения информации.

Буфер Обмена

Место в памяти, используемое для передачи информации. Информацию можно копировать в Буфер Обмена, а затем вставлять в другой документ, приложение или *Книгу обмена*.

Буфер экрана

Память, отводимая для отображения командной строки

В

Ветвь

Часть *дерева каталогов*, представляющая *каталог* и все его подкаталоги

Виртуальная память

Создаваемое с помощью страничных файлов *Windows NT* пространство на жестком диске, используемое в Windows NT в качестве фактической памяти. Преимущество страничной памяти — возможность выполнения большего числа приложений, чем допускается фактическим объемом физической памяти. Недостатки — уменьшение дискового пространства, занимаемого файлом подкачки, и снижение производительности

Владелец

Владелец файла или каталога полностью контролирует их и может изменять права доступа к ним. По умолчанию владельцем файла является создавший его пользователь. Владелец *ресурса* является лицом, использующее ресурс в данный момент.

Внешняя команда

Команда, хранящаяся в собственном файле и загружаемая с диска только при ее использовании.

Внутренняя команда

Команда, хранящаяся в файле CMD.EXE и находящаяся в памяти постоянно.

Время регистрации

В *Windows NT Server* — дни недели и время суток, в течение которых пользователь может регистрироваться в системе. По истечении времени регистрации пользователь может быть либо отключен, либо продолжит работу, но не сможет выполнять новых подключений.

Встроенные группы

Группы, входящие в *Windows NT Workstation* и *Windows NT Server* по умолчанию. Встроенные группы обладают набором *привилегий* и *прав*. В большинстве случаев встроенные группы удовлетворяют всем потребностям пользователей. Включая пользователей в те или иные группы, добиваются наличия у них необходимых привилегий. Группами управляют через *User Manager*.

Встроенный объект

Представляет информацию, созданную другим приложением. Информация встроенного объекта не существует за пределами документа, в который она встроена.

Вход контроля доступа (ACE)

Элемент в *списке контроля доступа (ACL)*. Вход содержит *идентификатор безопасности* пользователя (*SID*) и набор прав доступа. Процесс с совпадающим идентификатором имеет либо разрешающие права, либо запрещающие, либо разрешающие права с *аудитом*. Подробнее см. *Список контроля доступа*.

Г

Глобальная группа

В *Windows NT Server* *группа*, которая может использоваться в собственном *домене*, *серверах* и *рабочих станциях* домена и *доверяющих доменах*. Во всех случаях глобальная группа имеет предоставленные *права* и *привилегии* и может становиться членом *локальных групп*. Однако глобальная группа может содержать *учетные записи пользователей* только собственного домена. Глобальные группы обеспечивают способ создания удобных назначений для пользователя внутри домена. Эти назначения доступны как внутри, так и вне домена.

Глобальные группы не создаются и не поддерживаются *Windows NT Workstation*. Однако рабочие станции с *Windows NT Workstation*, входящие в домен, могут предоставлять глобальным группам домена права и привилегии для этих рабочих станций. Глобальные группы могут становиться членами локальных групп в этих рабочих станциях.

Глобальная учетная запись

В *Windows NT Server* обычная *учетная запись пользователя* в домашнем домене. Если в сети существует несколько доменов, то предпочтительно, чтобы каждый пользователь в сети имел только одну учетную запись и только в одном домене; доступ пользователя к *ресурсам* других доменов должен осуществляться через систему *доверительных отношений*.

Группа

В *User Manager* *учетная запись*, включающая в себя другие учетные записи, называемые членами группы. *Права и привилегии*, предоставленные группе, предоставляются и ее членам, что удобно для назначения общих свойств целому ряду учетных записей пользователей. В *Windows NT Workstation* группами управляют с помощью *User Manager*. В *Windows NT Server* — *User Manager for Domains*.

Группа программ

В *Program Manager* набор приложений. Группирование облегчает поиск приложений.

Д

Двухъярусная модель построения сети

Такая модель организации *доверительных отношений* между доменами, в которой все домены делятся на две категории: *домены учетных записей* и *ресурсные домены*. Все ресурсные домены доверяют доменам учетных записей, что делает возможным централизованное управление всей сетью.

Дерево каталогов

Графическое представление структуры *каталогов* на диске. Каталоги отображаются в виде *ветвей* дерева. Самый верхний каталог называется корневым.

Дескриптор безопасности

Атрибуты безопасности для *объекта*, такие как идентификатор владельца (*SID*), идентификатор *группы*, *список контроля доступа* (*ACL*) и системный список контроля доступа.

Динамический обмен данными (DDE)

Форма взаимодействия между процессами в семействе операционных систем Microsoft Windows. Две или более программы, поддерживающие динамический обмен данными, могут обмениваться между собой информацией и командами.

Динамически подключаемая библиотека (DLL)

Процедура *API*, доступ к которой из приложений осуществляется вызовом обычных процедур. Код этой процедуры не входит в исполняемый образ приложения. Операционная система автоматически изменяет исполняемый образ в процессе выполнения так, чтобы он указывал на DLL.

Диспетчер бюджета безопасности (SAM)

Защищенная подсистема *Windows NT*, поддерживающая *базу данных SAM* и вызывающая *API* для доступа к базе данных.

Доверительные отношения (Trust relationship)

Разновидность связи между *доменами*, предусматривающая выполнение *аутентификации*, когда пользователь, имея *учетную запись* только в одном домене, может обращаться ко всей сети. *Доверяющий домен* предоставляет право аутентификации *доверяемому домену*.

Доверяемый домен (trusted domain)

Домен, пользователи которого могут осуществлять доступ к *ресурсам* других, *доверяющих доменов*.

Доверяющий домен (trusting domain)

Домен, предоставляющий доступ к своим *ресурсам* пользователям других, *доверяемых доменов*.

Документ назначения

Документ, в который встраивается пакет или с которым связывается *объект*. Для встроенных объектов такой документ еще называют контейнерным документом.

Домашний каталог (Home directory)

Каталог, доступный для пользователя и содержащий файлы и программы этого пользователя. Домашний каталог может быть назначен либо каждому пользователю, либо нескольким пользователям сразу.

Домен

Для *Windows NT Server* это объединение нескольких компьютеров, использующих единую *базу учетных записей* и *политику безопасности*. Каждый домен имеет уникальное имя. См. также *Рабочая группа*.

Домен учетных записей (account domain)

В *двухъязычной модели построения сети* — домен, в котором хранятся учетные записи пользователей, но отсутствуют какие-либо *ресурсы*. Иногда называют Мастер-доменом. Противоположен *ресурсному домену*.

Драйвер принтера

Программа, управляющая взаимодействием принтера и компьютера.

Драйвер сетевого устройства

Программное обеспечение, координирующее взаимодействие между платой сетевого адаптера и оборудованием компьютера и другим программным обеспечением, а также управляющее физической работой сетевого адаптера.

Драйвер устройства

Программа, позволяющая определенному устройству взаимодействовать с *Windows NT*. Хотя устройство физически может быть установлено в компьютер, *Windows NT* не распознает его до тех пор, пока не будет установлен необходимый драйвер.

Дублирование диска

Установление зеркальной копии диска, подключенного к другому контроллеру. См. также *Зеркализация диска*.

Ж

Журнал

Файл с информацией о событиях защиты: попытках регистрации, попытках использования *ресурсов* и т.п. Создается функцией *audit* *Windows NT*.

Журнал приложений

Файл, содержащий ошибки, предупреждения и информацию, порожденные прикладными программами при включенном *audit* защиты *Windows NT*.

Журнал системы

Файл, содержащий ошибки, предупреждения и информацию, порожденные системой при включенном *audit* защиты *Windows NT*.

З

Зависимый сервис

Сервис, для работы которого требуется другой сервис. Например, *сервис Alerter* требует работы *сервиса Messenger*.

Загрузочный раздел

Раздел диска, отформатированный в *NTFS*, *FAT* или *HPFS* и содержащий файлы операционной системы *Windows NT* и файлы поддержки. Загрузочный раздел может совпадать с *системным разделом*.

Загрузчик

Определяет информацию, необходимую для запуска системы, например, о расположении файлов операционной системы. *Windows NT* автоматически исправляет конфигурацию и проверяет информацию при каждой загрузке системы.

Зеркализация диска

Создание идентичной копии раздела диска на другом диске.

Значимый элемент

Элемент *ключа* или подключа в *Регистре*.

И

Идентификатор безопасности (SID)

Уникальное имя, идентифицирующее зарегистрированного пользователя в *Windows NT*. SID может идентифицировать индивидуального пользователя или *группу*.

Именованный канал (named pipe)

Механизм взаимодействия между процессами, позволяющий одному процессу общаться с другим локальным или удаленным процессом.

Имя группы

Уникальное имя, идентифицирующее *локальную* или *глобальную группу* в *Windows NT*. Имя группы не может совпадать с именем другой группы или именем пользователя в своем *домене* или *рабочей станции*.

Имя домена

Имя, под которым *домен* известен в сети.

Имя компьютера

Уникальное имя длиной не более 15 латинских символов верхнего регистра, однозначно идентифицирующее компьютер в сети. Имя не может совпадать с именами других компьютеров или *именами доменов* и не должно содержать пробелов. Если применяются протоколы *TCP/IP* и *DNS*, в имени вместо знака подчеркивания используется дефис.

Имя пользователя

Уникальное имя, идентифицирующее *учетную запись пользователя* в *Windows NT*. Имя пользователя не может совпадать с именами других пользователей или *групп* в *домене* или на *рабочей станции*.

Интерактивная регистрация

Пользователь должен ввести информацию с клавиатуры компьютера в диалоговое окно, изображенное на экране. *Windows NT* предоставит или отвергнет доступ в зависимости от информации, введенной пользователем. Противоположна *удаленной регистрации*.

Интерактивная регистрация с использованием канала удаленного доступа

В *Windows NT 4.0* пользователь может зарегистрироваться в *домене*, даже когда компьютер не подключен к локальной сети. При этом можно подключиться к удаленному домену в процессе *аутентификации* средствами удаленного доступа (например, по модему). *Контроллер* удаленного домена *Windows NT* предоставит или отвергнет доступ в зависимости от информации, введенной пользователем. Противоположна *удаленной регистрации*.

Интерфейс прикладного программирования (API)

Набор функций, используемых прикладными программами для запросов и исполнения операционной системой низкоуровневых сервисов.

Интерфейс NetBIOS

Интерфейс программирования, позволяющий посылать и принимать запросы ввода/вывода удаленного компьютера. Скрывает техническую часть сети от программ.

Источник бесперебойного питания (UPS)

Источник питания со встроенными батареями, подключенный к компьютеру и используемый при сбоях напряжения питания.

Исходный документ

Документ, в котором создан связанный или внедренный *объект*.

Исходный каталог

Каталог, содержащий файлы, которые надо скопировать или переместить.

К

Каталог

Часть структуры, служащей для организации хранения файлов на диске. В каталоге могут храниться файлы и другие каталоги.

Каталог назначения

Каталог, в который Вы собираетесь скопировать или перенести файлы.

Кластер

Группа независимых систем, работающих как единое целое. Кластеры используются для повышения надежности доступа к хранимой информации и для повышения вычислительной мощности.

Клиент

Компьютер, осуществляющий доступ к *ресурсам* другого компьютера (называемого *сервером*), предоставленным в совместное использование.

Ключ

В *реестре* одно из четырех поддеревьев. Каждый ключ может содержать значимые величины и другие подключи. В реестре ключ аналогичен *каталогу*, а значимая величина — файлу.

Книга обмена

Место постоянного хранения информации, которую надо сохранить или предоставить для совместного использования. Отличается от *Буфера Обмена*, служащего для временного хранения информации. Текущее содержимое Буфера Обмена можно поместить в *Книгу обмена* с помощью ClipBook Viewer. После этого информацию можно предоставить в совместное использование. См. *Страница Книги обмена*.

Командный файл

Неформатированный текстовый файл, содержащий одну или несколько команд *Windows NT*. Командный файл имеет расширения .CMD или .BAT. При запуске команды в командном файле выполняются последовательно.

Компьютеры импорта

При *тиражировании каталогов* — *серверы* или *рабочие станции*, на которые передаются копии главного набора файлов и *каталогов с сервера экспорта*.

Контейнерный объект

Объект, логически содержащий другие объекты. Например, *каталог* — это контейнерный объект, содержащий логически другие каталоги и файлы. Файл не является контейнерным объектом.

Контроль

Любой механизм, ручной или автоматический, обеспечивающий безопасность имущества или позволяющий процессу выполняться так, как задумано.

Контроллер домена

Сервер, имеющийся в каждом *домене Windows NT Server*, на котором происходит *авторизация* всех регистраций, а также поддерживается *политика безопасности*.

Крайняя привилегия

Принцип, по которому пользователи должны обладать только минимумом *привилегий*, необходимым для выполнения их работы.

Кэширование диска

Метод, используемый для повышения производительности файловой системы. Вместо того, чтобы постоянно обращаться к диску для выполнения операций чтения и записи, файлы хранятся в кэше в памяти. Все операции чтения/записи выполняются со скоростью обращения к памяти, что значительно быстрее, чем скорость обращения к диску.

Л

Логический диск

Подраздел расширенного раздела жесткого диска.

Локальная группа

В *Windows NT Workstation* — группа, которой можно предоставлять *права и привилегии* исключительно для *рабочей станции*. Однако она может включать *учетные записи пользователей* того же компьютера и (если рабочая станция входит в *домен*) *учетные записи пользователей* и *глобальные группы* домашнего и *доверяемых доменов*. Локальные группы предоставляют способ создания объединений пользователей как этой рабочей станции, так и нет, для применения только на рабочей станции.

В *Windows NT Server* — группа, которой можно предоставлять права и привилегии исключительно внутри домена. Но в нее могут входить *учетные записи пользователей* и *глобальные группы* домашнего и *доверяемых доменов*. Локальные группы предоставляют способ создания объединений пользователей как этого домена, так и нет, для применения только на серверах домена.

Локальная учетная запись

Учетная запись такого пользователя в *домене*, чья *глобальная* учетная запись находится не в *доверяемом домене*. Если установлены *доверительные отношения*, применение локальных учетных записей не требуется.

Локальный принтер

Принтер, подключенный непосредственно к одному из портов компьютера.

Локальный профиль

Файл, содержащий информацию о параметрах окружения пользователя, например сетевых подключениях, группах программ, положении и размерах окон, сохраняемых при выходе пользователя из *Windows NT Workstation*. Локальные профили сохраняются там же, где и база данных *реестра*.

М

Максимальный срок жизни пароля

Период времени, в течение которого можно использовать *пароль*, прежде чем система потребует его изменить. См. также *Политика ведения учетных записей*.

Маска доступа

Определяет все возможные действия, применимые к определенному типу *объекта*, во *входе контроля доступа*. *Права* предоставляются или запрещаются на основе маски.

Мастер-домен

Модель организации *даменов*, в которой все *учетные записи* доменов находятся в одном домене. Позволяет централизованно управлять учетными записями. Иногда называется *доменом учетных записей*.

Минимальный срок жизни пароля

Период времени, в течение которого будет использоваться установленный *пароль*, прежде чем его можно будет изменить. См. также *Политика ведения учетных записей*.

Многопротокольная маршрутизация (MPR)

MPR содержит функции маршрутизации RIP (Routing Information Protocol) и позволяет использовать *Windows NT Server* в качестве маршрутизатора между двумя или несколькими сетями с использованием RIP на IP, IPX или на том и другом одновременно. Компьютер может выступать также как агент передачи DHCP (DHCP Relay agent), что позволяет транслировать сообщения DHCP по сети IP.

Н

Нарушитель

Неавторизованный пользователь.

Неактивная учетная запись пользователя

Учетная запись пользователя, которому запрещено регистрироваться. Эта учетная запись появляется в списке учетных записей в *User Manager* и может быть активизирована в любое время.

О

Обязательный профиль пользователя

Профиль пользователя, созданный администратором и назначенный одному или нескольким пользователям. Обязательный профиль пользователя — файл с расширением .MAN, в который записываются параметры окружения пользователя. Обязательный профиль не может быть изменен пользователем и остается неизменным при каждой регистрации.

Обратная связь

Механизм, используемый *серверам удаленного доступа*. После установления первичного соединения удаленного пользователя с сервером связь разрывается, и сервер перезванивает клиенту по предварительно заданному номеру телефона или по номеру, сообщенному удаленным клиентом. Используется для повышения защищенности сети, а также для сокращения расходов удаленного клиента.

Объект

1. Отдельный экземпляр, имеющий объектный тип; управляется только с использованием *сервиса*, примененного к объектам данного типа. 2. Любой фрагмент информации, созданный Windows-приложением с помощью *связи и внедрения объектов* (OLE), что позволяет ему быть связанным или внедренным в любой объект.

Описатель объекта

Включает информацию управления доступом и непосредственно указатель на *объект*. Прежде чем процесс сможет управлять объектом *Windows NT*, он должен получить описатель объекта через диспетчер объектов.

Отказоустойчивость

Способность компьютера и операционной системы адекватно реагировать на катастрофические события (например, пропадание напряжения или отказ техники). Обычно под отказоустойчивостью понимается способность системы продолжать функционировать без потери данных или закрытие системы с перезапуском и последующим восстановлением всех процессов, присутствовавших до момента аварии.

П

Пароль

Уникальная строка символов, вводимая для *авторизации* доступа при регистрации. Важное средство защиты, пароль служит для ограничения входа в систему и доступа к компьютерным системам и *ресурсам*.

Первичный раздел

Часть физического диска, которая может быть помечена для использования операционной системой. На каждом физическом диске может быть до 4 первичных разделов (или до трех, если имеется расширенный раздел). Первичный раздел не может быть разбит на подразделы.

Переменная окружения

Строка, содержащая информацию об окружении системы (например, о диске, пути или имени файла), ассоциированном с символьным именем, которое используется системой *Windows NT*. Для определения переменных окружения применяется опция System в Панели управления или команда **set**.

Персональный профиль пользователя

В *Windows NT Server* *профиль*, созданный администратором и назначенный одному пользователю. В персональный профиль записываются все изменения, сделанные пользователем в течение сеанса работы. Эти изменения сохраняются при выходе пользователя из системы. При последующей регистрации на любой *рабочей станции* с *Windows NT Workstation* загружается персональный профиль (файл с расширением .USR) и выставляются те параметры окружения, что были перед окончанием предыдущего сеанса.

Подключенный пользователь

Пользователь, осуществляющий доступ к *ресурсам* компьютера по сети.

Политика аудита

Определяет тип регистрируемых событий, происходящих в *дамене* или на отдельном компьютере. Также определяет действия, которые должна выполнить система *Windows NT* при переполнении *журнала регистрации*.

Политика безопасности

В *Windows NT Workstation* политика безопасности состоит из *политики ведения учетных записей*, политики привилегий пользователей и *политики аудита*. Управление через *User Manager*.

В *Windows NT Server* политика безопасности состоит из политики ведения учетных записей, политики привилегий пользователей, политики аудита и политики *доверительных отношений*. Управление через *User Manager for Domains*.

Политика ведения учетных записей

Устанавливает способ применения *паролей* *учетными записями* всех *пользователей* в *дамене* или на отдельном компьютере.

Полное имя

Полное имя пользователя, обычно состоящее из имени, фамилии и отчества. Полное имя является частью информации, с которой оперирует *User Manager* при определении *учетных записей* *пользователей*.

Порт

Разъем или гнездо для подключения к компьютеру таких устройств, как принтеры, мониторы или модемы. Информация передается от компьютера к устройству по кабелю.

Последняя известная работоспособная конфигурация

Совокупность параметров управления, являющаяся точной копией последних параметров управления, использовавшихся при успешной загрузке компьютера.

Право доступа

Разрешение процессу определенным образом воздействовать на определенный *объект*. Различные типы объектов поддерживают различные права доступа, хранящиеся в *списках контроля доступа*.

Предоставление файлов в совместное использование

Способность *Windows NT Workstation* и *Windows NT Server* использовать часть (или всю) своей локальной файловой системы совместно с другим компьютерами.

Привилегия

Позволяет пользователю выполнять определенные действия в системе. Привилегии предоставляются системе в целом в отличие от *прав доступа*, применимых к определенным *объектам*.

Приложения для MS-DOS

Приложения, разработанные для MS-DOS и поэтому не способные использовать все преимущества *Windows NT*.

Приложение не для Windows NT

Относится к приложениям, разработанным для Windows 3.x, MS-DOS, OS/2 или POSIX, но не специально для *Windows NT*, что не позволяет им реализовать все преимущества *Windows NT*.

Принтер по умолчанию

Принтер, на который выполняется печать из приложения без предварительного выбора принтера. Можно установить только один принтер по умолчанию; это должен быть наиболее часто используемый принтер.

Проверка

См. *Проверка доступа*.

Проверка доступа

Проверка информации об *учетной записи пользователя* для определения возможности предоставления субъекту права выполнения запрашиваемой операции.

Программа-мастер

Специальная программа, предназначенная для облегчения выполнения каких-либо рутинных операций. Использует пошаговый подход к выполнению последовательности действий, не позволяя пропустить ввод или определение каких-либо важных параметров. В *Windows NT Server 4.0* несколько программ-мастеров — все они вызываются из специальной консоли *Administrative Wizards*.

Протокол

Набор правил и соглашений, используемых двумя компьютерами для передачи сообщений по сети. Сетевое программное обеспечение обычно использует несколько уровней протоколов, расположенных один над другим.

Профиль пользователя

Информация о конфигурации, отсортированная по пользователям и сохраняемая в профиле пользователя. Информация включает все параметры окружения для определенного пользователя или *группы*. К параметрам окружения относятся, например, размещение окон и значков на *рабочей поверхности*, цвета экрана, программа сохранения экрана, сетевые подключения, подключенные принтеры т.п. При регистрации пользователя *Windows NT* конфигурируется в соответствии с профилем. В *Windows NT 4.0* профили пользователей можно редактировать с помощью редактора системной политики — *System Policy Editor*.

Профиль умолчания

См. *Профиль умолчания пользователя* и *Системный профиль умолчания*.

Профиль умолчания пользователя

На *Windows NT Server* — профиль, загружаемый *сервером*, когда: 1. профиль, назначенный пользователю, не может быть загружен; 2. пользователь, не имеющий *персонального профиля*, регистрируется на компьютере впервые; 3. пользователь регистрируется как гость.

Путь

Указывает положение файла внутри *дерева каталогов*.

Путь импорта

При *тиражировании каталогов* — *путь* приема файлов и каталогов.

Путь сценария регистрации

При регистрации пользователя компьютер, выполняющий *авторизацию*, выполняет поиск *сценария регистрации* (если он был назначен) в *пути*, заданном на локальном компьютере. Обычно это C:\WINNT35\SYSTEM32\REPL\IMPORT\SCRIPTS.

Путь экспорта

При *тиражировании каталогов* — *путь* на *сервере экспорта*, каталоги и файлы из которого автоматически экспортируются на другие *серверы*.

Р

Рабочая группа

Применительно к *Windows NT* рабочая группа представляет собой совокупность компьютеров, сгруппированных для удобства просмотра их сетевых ресурсов.

Рабочая поверхность

Фоновая поверхность экрана, над которой располагаются окна, значки и диалоговые окна. В *Windows NT 4.0* на рабочей поверхности постоянно располагаются такие значки, как *My Computer*, *Network Neighborhood*, *Recycle bin*.

Рабочая станция

Компьютеры, на которых исполняется *Windows NT Workstation*, называются рабочими станциями в отличие от серверов, на которых выполняется *Windows NT Server*.

Рабочий стол

См. *Рабочая поверхность*

Распорядитель локальной безопасности (LSA)

Создает маркер безопасного доступа для каждого пользователя, обращающегося к системе.

Расширение

Точка и до 3 символов в конце имени файла. Расширение обычно указывает на тип файла.

Редактор реестра (Registry Editor)

Приложение, входящее в систему *Windows NT* и позволяющее просматривать и редактировать записи в реестре.

Редиректор

Сетевая программа, принимающая запросы ввода/вывода для удаленных файлов, именovaných каналов или почтовых слотов и передающая их сетевым сервисам на другом компьютере. В *Windows NT* редиректоры выполнены как драйверы файловой системы.

Реестр

Архив баз данных *Windows NT*, хранящий информацию о конфигурации компьютера, включая аппаратные средства, установленное программное обеспечение, установки окружения и др.

Ресурс

Любая часть компьютерной системы или сети (например, диск, принтер, память), которая может быть предоставлена программе или процессу во время работы.

Ресурсный домен

В двухъярусной модели построения сети — домен, не содержащий ни одной учетной записи пользователей сети (кроме администратора) и располагающий ресурсами, предоставленными в совместное использование. Противоположен по функциям домену учетных записей.

С

Свободное пространство

Неиспользуемая и неотформатированная часть жесткого диска, которая может быть разбита на разделы или подразделы. Свободное пространство внутри расширенного раздела доступно для создания логических дисков. Свободное пространство, не используемое расширенным разделом, доступно для создания раздела. Максимальное число разделов — четыре.

Связанный объект

Представление позиции объекта, вставленного в документ. Объект при этом существует в отдельном файле, и при его изменении связанный объект отображает эти изменения.

Связь и внедрение объектов (OLE)

Способ передачи и обмена информацией между приложениями.

Сервер

В *Windows NT Workstation* компьютер, предоставляющий свои ресурсы для совместного использования в сети. См. также Клиент.

В *Windows NT Server* компьютер, содержащий копию базы данных защиты домена и идентифицирующий регистрацию по сети. См. также Контроллер домена.

Сервер экспорта

При тиражировании каталогов — сервер, с которого тиражируется основной набор каталогов на указанные серверы или рабочие станции в этом или других доменах.

Серверный профиль

Файл, содержащий параметры окружения пользователя и расположенный на локальном диске или в совместно используемом каталоге. Обязательный, персональный и профиль умолчания являются серверными профилями.

Сервис

Процесс, выполняющий определенные функции системы и часто предоставляющий API для вызова других процессов. Сервисы *Windows NT* поддерживают RPC, что подразумевает возможность вызова процедур API с удаленных компьютеров.

Сервис планирования

Поддерживает и требуется для использования команды **at**, которая позволяет назначать исполнение программ и команд на указанное время и дату.

Сервис Event Log

Записывает указанные *события* в журналы системы, защиты или приложений.

Сервис File Replication

Сервис, выполняющий *тиражирование данных*.

Сервис Messenger

Посылает и принимает сообщения, рассылаемые администраторами или *сервисом Alert*.

Сервис NetDDE

Обеспечивает транспорт и защиту для *динамического обмена данными* между компьютерами

Сервис Netlogon

В *Windows NT Server* определяет правильность регистрации в *домене*, а также синхронизирует базу данных домена между *контроллером домена* и другими *серверами Windows NT* в домене.

Сервис RPC

Сервис вызова удаленных процедур, используемый подсистемой RPC.

Сервис Server

Поддерживает *вызов удаленных процедур*, а также предоставление в совместное использование файлов, принтеров и *именованных каналов*.

Сервис Workstation

Сервис Windows NT, предоставляющий функции *API*, управляющие *редиректорам Windows NT*. Обеспечивает сетевые подключения.

Сетевой каталог

См. *Совместно используемый ресурс*.

Системный профиль умолчания

В *Windows NT Server* профиль, используемый при работе системы, когда в ней не зарегистрировался ни один пользователь. Диалоговое окно Welcome означает, что используется системный профиль умолчания.

Системный раздел

Том, содержащий необходимые для загрузки *Windows NT* файлы, зависящие от типа техники.

Событие

Любое значительное происшествие в системе или в приложении, о котором необходимо оповестить пользователя или занести запись в журнал.

Совместно используемый ресурс

Ресурс (каталог, принтер, страница Книги обмена и т.п.), доступный пользователям сети.

Специальные группы

Группы, члены которых не назначаются администратором. Пользователь становится членом такой группы при выполнении определенных действий в сети. Например, пользователь, выполнивший *интерактивную регистрацию*, принадлежит к специальной группе Interactive.

Список контроля доступа (ACL)

Часть дескриптора защиты, перечисляющая защитные функции, примененные к *объекту*. *Владелец* объекта, обладающий *контролем* над объектом, может изменять список контроля доступа к объекту для предоставления или запрещения доступа к объекту другим. Список контроля доступа состоит из *входов контроля доступа*.

Страница Книги обмена

Единица информации, размещенная в локальной *Книге обмена*. Страница постоянно сохраняется. Информация со страницы может быть скопирована в *Буфер Обмена* и затем в документы, а также может быть предоставлена для совместного использования в сети.

Субъект

Комбинация маркера *контроля* доступа пользователя и программы, действующей от имени этого пользователя. В *Windows NT* субъекты применяются для отслеживания и управления правами программ, выполняемых различными пользователями.

Сценарий регистрации

Обычно командный файл. Сценарий регистрации автоматически выполняется при каждой регистрации пользователя в системе. Может применяться для настройки окружения пользователя или рабочей среды. Сценарий регистрации назначается одному или нескольким пользователям сразу.

T

Тиражирование каталогов

Автоматическое копирование главного набора *каталогов с сервера* (называемого сервером экспорта) на выбранные серверы или *рабочие станции* (называемые компьютерами импорта) в том же или другом *дамене*. Тиражирование упрощает поддержание идентичности наборов каталогов на нескольких компьютерах, так как следить надо только за главным набором. Файлы тиражируются всякий раз при добавлении в каталог экспорта или при сохранении в них изменений. См. также *Directory Replicator service*.

Том

Раздел диска или несколько разделов, отформатированных для использования файловой системой.

Транспорт NetBEUI

См. *NetBEUI*.

Транспорт TCP/IP

См. *TCP/IP*.

У

Удаленная регистрация

Когда пользователь устанавливает связь с удаленного компьютера, проверка доступа осуществляется на компьютере, не имеющем маркера доступа для данного пользователя. (Маркеры доступа создаются при *интерактивной регистрации*.)

Удаленное администрирование

Администрирование компьютера с другого компьютера, связанного с первым по сети. Удаленно можно администрировать компьютер, работающий в *Windows NT* с клиентов, на которых исполняется Windows for Workgroups, Windows 95 или Windows NT.

Удаленный доступ

Доступ к компьютеру или сети с использованием каналов связи. В качестве каналов могут выступать обычные телефонные линии, выделенные линии, сети X.25 или ISDN. Используется для подключения мобильных пользователей или связи двух локальных сетей между собой. В Windows NT 4.0 поддерживается связь по линии RS232 (нуль-модем) или с использованием протокола *PPTP*.

Улей

Дискретный набор *ключей*, подключей и значений, находящийся сверху иерархии реестра. Улей поддерживается одиночным файлом и файлом LOG, находящимися в каталоге %systemroot%\system32\config

Уникальность пароля

Число *паролей*, которые необходимо сменить, прежде чем сможет быть использован первоначальный пароль. См. также *Политика ведения учетных записей*.

Управляющий набор

Полный набор параметров устройств и *сервисов*, записанный в *реестре* в ключе HKEY_LOCAL_MACHINE\SYSTEM.

Учетная запись пользователя

Содержит всю информацию о пользователе *Windows NT*. Включает в себя *имя пользователя* и *пароль*, необходимые для регистрации, *группы*, в которые входит данная учетная запись, *права* и *привилегии* пользователя при работе в системе и доступе к *ресурсам*. В *Windows NT Workstation* учетные записи пользователей редактируются с помощью *User Manager*, в *Windows NT Server — User Manager for Domains*. В *Windows NT 4.0* для создания новых учетных записей можно использовать *программу-мастер* Add User Account Wizard.

Ф

Файловая система

Общая структура именования, хранения и организации файлов в операционной системе.

Файловая система FAT

Базируется на таблице размещения файлов, обслуживаемой операционной системой и отслеживающей состояние различных сегментов диска, используемых для хранения файлов.

Файловая система HPFS

Высокопроизводительная файловая система, изначально использовавшаяся в *OS/2* версии 1.2 и позже. Поддерживает длинные имена файлов, но не поддерживает функций защиты. В *Windows NT 4.0* не поддерживается.

Файловая система NTFS

Улучшенная файловая система, разработанная специально для *Windows NT*. Поддерживает средства восстановления файловой системы, допускает использование чрезвычайно больших носителей данных, а также различных функций подсистемы POSIX. Поддерживает объектно-ориентированные приложения, обрабатывая все файлы как объекты с определяемыми пользователем и системой атрибутами.

Физическая защита

Осуществляет контроль за физическим доступом к носителям информации, прерываниям *сервисов*, повреждением программ или данных и нелегальным разглашением информации.

Ч

Чередование дисков

Запись данных полосками по всему тому, созданному из участков *свободного пространства* от 2 до 32 дисков.

Членство в группе

Принадлежность к *группе*. *Права и привилегии*, предоставленные группе, распространяются на ее членов. В большинстве случаев действия, которые может совершить пользователь *Windows NT*, определяются принадлежностью к той или иной группе.

Ш

Шифрование данных

Изменение формата данных, так чтобы их нельзя было прочитать.

А

ACE

См. *Вход контроля доступа*.

ACL

См. *Список контроля доступа*.

Administrative Wizards

Единая консоль управления административными *программами-мастерами* в *Windows NT Server 4.0*. Объединяет такие программы, как Add User Account (Добавление новой учетной записи пользователя), Group Management (Управление группами), Managing File and Folder Access (Управление доступом к файлам и папкам), Add printer (Добавление принтера), Add/Remove Programs (Добавление/удаление программ), Install New Modem (Установка нового модема), Network Client Administrator (Администратор сетевых клиентов), License Compliance (Соответствие лицензий).

Alerts

Сервис, предупреждающий пользователей и компьютеры об *административных сигналах тревоги* в компьютере. Используется *сервисом Server* и другими. Требует функционирования *сервиса Messenger*.

API

См. *Интерфейс прикладного программирования*.

C

Call-back

См. *Обратная связь*.

ClipBook service

Поддерживает работу *Книги обмена*. Позволяет предоставлять информацию в совместное использование.

D

DDE

См. *Динамический обмен данными*.

Directory Replicator service

Тиражирует *каталоги* и файлы в них на другие компьютеры.

Directory Service Manager for Netware (DSMN)

Дополнительный сетевой *сервис*, позволяющий синхронизировать между собой *учетные записи домена* NT Server и учетные записи одного или нескольких *серверов* Netware версий 2.x и 3.x, как бы включив их в один домен. После такой синхронизации пользователи домена *Windows NT* получают прозрачный доступ к *ресурсам* серверов Netware и имеют одинаковые *права и привилегии, имена, учетные записи и пароли*.

F

FAT

См. *Файловая система FAT*.

File and Print Services for Netware (FPNW)

Сервис Windows NT Server, позволяющий эмулировать работу *сервера* Netware 3.x. В результате клиенты Netware могут без каких-либо изменений осуществлять доступ к *ресурсам* NT Server и управлять им.

FTP

Протокол передачи данных File Transfer Protocol (FTP) позволяет перемещать файлы с одного компьютера в Internet на другой. *Серверы*, предназначенные для предоставления файлов для загрузки на другие компьютеры, называются серверами FTP.

G

Gateway Service for Netware

Сервис Windows NT Server, позволяющий предоставлять прозрачный доступ клиентам сети Microsoft к *ресурсам* сервера Netware через шлюз. Шлюзование позволяет не использовать на клиентах протокол IPX.

Gopher

По сути, это меню *ресурсов* Internet. Для управления ими используются *серверы* Gopher.

H

HCL

Список совместимого оборудования. В нем перечислены как конечные системы, так и отдельные компоненты, с которыми была проверена работа в *Windows NT*.

HPFS

См. *Файловая система HPFS*.

I

Internet Information Server (IIS)

Информационный *сервер* Microsoft, работающий под управлением *Windows NT Server*. Начиная с NT Server версии 4.0, является составной частью системы. Включает в себя серверы *Web*, *Gopher* и *FTP*.

L

LSA

См. *Распорядитель локальной безопасности*.

M

MPR

См. *Многопротокольная маршрутизация*.

N

NetBEUI

Первичный протокол локальной сети NetBIOS Extended User Interface используется в *Windows NT*.

NetBIOS

См. *Интерфейс NetBIOS.*

NTFS

См. *Файловая система NTFS.*

P**PPTP**

Point-to-Point-Tunneling Protocol — механизм защищенной передачи данных через Internet между двумя локальными сетями. Организуется “тоннель” через который направляются пакеты IP, IPX или *NetBEUI*. Этот механизм реализован в *Windows NT*, начиная с версии 4.0.

R**RAS**

См. *Удаленный доступ.*

RPC

См. *Сервис RPC.*

S**SAM**

См. *Диспетчер бюджетов безопасности.*

SID

См. *Идентификатор безопасности.*

System Policy Editor

Редактор системной политики в *Windows NT Server 4.0*. Позволяет вносить изменения в *реестр* как непосредственно, так и через файлы политики. Управляет практически всеми настройками *серверов* и клиентов, входящих в *домен*, а также *профилями* отдельных *пользователей*. В качестве клиентов поддерживаются используемые *Windows NT* или *Windows 95*.

T**TCP/IP**

Transmission Control Protocol/Internet Protocol. Первичный протокол глобальных сетей, используемый в *Windows NT* для взаимодействия с системами в сетях TCP/IP и для доступа к электронным доскам объявлений и почтовым службам, работающим под UNIX.

U

UPS

См. *Источник бесперебойного питания*.

User Manager

Инструмент обеспечения защиты *Windows NT Workstation*. Позволяет администрировать *учетные записи* пользователей, *групп* и политику защиты.

User Manager for Domains

Инструмент *Windows NT Server*, обеспечивающий защиту как отдельного компьютера, так и *домена*. Позволяет администрировать *учетные записи пользователей*, *групп* и политику защиты.

W

Web-сервер

См. *World Wide Web*.

Windows NT

Переносимая, защищенная 32-разрядная операционная система, обладающая приоритетной (вытесняющей) многозадачностью, из семейства Microsoft Windows. Выпускается в двух версиях: *Windows NT Workstation* и *Windows NT Server*.

Windows NT Server

Версия *Windows NT*, предназначенная для использования в качестве *сервера*. Может выполнять роль *контроллера домена* или просто сервера.

Windows NT Workstation

Версия *Windows NT*, предназначенная для использования в качестве *рабочей станции*. У *Windows NT Workstation* отсутствуют средства администрирования доменов и нет возможности *аутентификации* пользователей доменов.

World Wide Web (WWW)

Сервер, на котором хранятся мультимедиа-документы, связанные между собой гипертекстовыми ссылками. Просмотр документов осуществляется с помощью специальных программ. Переход от одного документа к другому выполняется щелчком ссылки.

WWW

См. *World Wide Web*.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

А

автоматическая регистрация	72
авторизация <i>см. также</i> аутентификация	
— сквозная	83
администрирование	
— домена	3
аутентификация	63, 141, 259

В

владелец	101, 165, 339
владение каталогами и файлами	173
выбор	
— профиля техники	201
— работоспособной конфигурации	200

Г

группа пользователей	88
— встроенные глобальные	93
— встроенные локальные	91
— глобальные	92, 97-98
— локальные	89, 91, 95, 98
— на рабочих станциях	91
— рабочая	2
— создание и модификация	95
— специальные	99
— Creator Owner	101
— Everyone	100
— Interactive	100
— Network	100

Д

доверительные отношения	7
— типы	7
— требования к серверу	23
домашний каталог	120
домен	3
— нагрузочная способность	6
— учетных записей	8

доменные модели	10
— однодоменная	10
— полностью доверительные отношения ..	16
— практическая реализация	17
— с несколькими мастер-доменами	14
— с одним мастер-доменом	11
доступ к объекту	
— к серверам Netware	226
— списки контроля доступа	77

Ж

жесткий диск	
— замена секторов	195
— определение объема	35
— проверка состояния	191,
— разделы диска	162

З

зеркализация серверов	203
— система Octopus	204

И

идентификатор защиты	63
источники бесперебойного питания	199

К

кластеры	205
— архитектура	208
— на основе Windows NT Server	210
контроллер домена	30
— первичный	3
— повышение статуса	4
— резервный	3, 5, 46

Л

лицензия	
— планирование	39
— “хранящаяся на клиенте”	40
— “хранящаяся на сервере”	39
— Microsoft BackOffice	41

М	
маркер доступа	63, 76
маршрутизация	243
— между локальными сетями	245
— многопротокольная	244
— статическая	246
— через коммутируемый канал связи	247
минимальная защита	
— программная	284
— физическая	284
модель	
— доменов	2, 10
— рабочих групп	2
— безопасности	58
О	
оперативная память	
— выбор	33
П	
пароль пользователя	85
персональный доступ	
— к принтерам	74
— к файлам и каталогам	74
— элементы управления	73
— User Manager for Domains	75
планирование	26
— выбор процессора	36
политика ведения учетных записей	144
— блокировка рабочей станции	148
— блокировка учетных записей	147
— время неизменности пароля	146
— минимальная длина пароля	146
— обязательность регистрации	148
— отключение пользователей	148
— срок жизни пароля	145
— хранение истории паролей	147
права	101
права доступа к файлам и каталогам	165
— на NTFS	177
— предоставление	166
— стратегия предоставления	174
— File Delete Child	175
предупреждение	
о легальности использования	64
привилегии	101, 102
— встроенных локальных групп	106
— встроенных учетных записей	104
— изменение	111
— Account Operators	110
— Administrator	105
— Administrators	108
— Backup Operators	109
— Guest	104
— Guests	109
— Power Users	107
— Print Operators	110
— Server Operators	109
— Users	106
принтер	214
— защита реестра	222
— настройки	217
— создание	214
профили пользователей	113
— домашние каталоги	120
— обязательные	115
— ограничение времени работы	123
— ограничение числа рабочих станций ..	124
— персональные	115
— умолчания	115
— системный умолчания	115
— создание и редактирование	116
— сохранение	118
Р	
регистрация	62
— в Windows NT 4.0	65
Редактор системной политики	125
реестр	222
— назначение	276

— ограничение доступа	280
— структура	276
— улы и файлы	279
резервное копирование	195
— Arcada Backup Exec	197
— Cheyenne ARCserve	198
— Palindrome Backup Director	199

С

сервер	3
— вспомогательных служб	29
— печати	28
— приложений	28
— удаленного доступа	29
сетевые протоколы	37, 46
система защиты	
— Менеджер защиты учетных записей	59
— Распорядитель локальной безопасности	59
— Справочный монитор безопасности ...	61
системная политика	
— загрузка	130
— к группам	131
— к компьютерам	126
— к пользователям	126
— параметры	133, 137
— редактирование	127
— шаблоны	142
совместное использование	
— принтеров	216
— файлов и каталогов	178
список совместимого оборудования	32
сценарии регистрации	122

Т

технология RAID	192
— зеркализация и дублирование дисков ..	193
— чередование дисков	192
— RAID2	194
— RAID5	194

тиражирование каталогов	183
— защита	186

У

удаленный доступ	242
— аутентификация	259
— возобновление связи	266
— доменная основа защиты	256
— обратная связь	260
— ограничение доступа	262
— отключение пользователей	261
— параметры дозвона	67-71
— параметры регистрации	67
— привилегия	257
— шифрование данных	263
уровень C2	54
— Оранжевая книга	55
— сертификация Windows NT	55
— требования	54
установка	42
— видеоадаптера	49
— выбор роли сервера	46
— графическая часть	45
— на большое число компьютеров	50
— национальные параметры	45
— неграфическая часть	44
— способ	43
учетная запись	80
— глобальная	80
— локальная	80
— назначение	82
— общие параметры	143
— программа-мастер	87
— создание и редактирование	84

Ф

файловая система	36, 152
— длинные и короткие имена файлов ...	158
— компрессия файлов и каталогов	160

— преобразование существующего раздела	164	— односторонний доступ	270
— FAT	153	IPX/SPX	
— HPFS	154	— конфигурирование	48
— NTFS	156, 232	Machintosh	38
файл-сервер	27	Netware	224
CHKDSK	191	— миграция на Windows NT	236
DHCP-сервер	47	— организация доступа к Windows NT ...	230
DNS Server	47	— организация шлюза	228
Emergency Repair Disk	202	— сервер взаимодействия	30
FORMAT	163	— централизованное управление серверами	233
Group management Wizard	99	Server Manager	4
HCL	32	SID см. Маркер доступа	
Internet		TCP/IP	
— локальная сеть как ресурс	271	— конфигурирование	48

Федор Зубанов в 1984 году с красным дипломом окончил МИРЭА по специальности, далекой от персональных компьютеров, — инженер-оптик-исследователь. Потом работал в НИИ, учился в аспирантуре, но был врасплох застигнут ветрами перемен. Перестроился: резко порвав с прежней специальностью, связал дальнейшую судьбу с персональными компьютерами и компанией Microsoft.

Около года в СП «Диалог» занимался поддержкой программных продуктов, а затем с группой энтузиастов перешел в фирму РПИ, представлявшую тогда интересы Microsoft в СССР. Здесь начал вплотную работать с системой Windows и приложениями для нее, проявляя особенный интерес к проблемам поддержки русского языка, что привело в итоге к системе многоязычной поддержки для Windows R-Win, написанной совместно с приятелем. Приложил руку и к локализации Windows 3.1, Excel 4.0 и Works для Windows 2.0. В качестве хобби программирует на VB, о чем поведал миру в серии статей в журнале *Компьютер-Пресс*. В качестве специалиста по продуктам для Windows его пригласили в представительство Microsoft в России. С появлением Windows NT сердце Федора бесповоротно было отдано этой операционной системе.

Он часто выступает на семинарах и выставках, пишет статьи для изданий Microsoft АО, как технический редактор ведет Российскую страницу на сервере Web Microsoft (www.microsoft.com), постоянно общается с крупными заказчиками и старается им помочь.

E-mail: FyodorZ@aomicrosoft.msk.su

Федор Зубанов
Windows NT — выбор "профи"

Главный редактор **А. И. Козлов**
Главный менеджер **М. И. Царейкин**

Редактор **А. А. Кунарев**
Технический редактор **И. В. Васильева**

Оригинал-макет выполнен с использованием
издательской системы Aldus PageMaker 5.0
Компьютерный дизайн: **Е. В. Белоусова, Д. В. Петухов**

Подготовлено издательским отделом "Русская Редакция"
ТОО "Channel Trading Ltd."
Генеральный директор **В. В. Телушкин**

Лицензия ЛР № 090082 от 14.04.94 г.
Подписано в печать 22.07.96 г. Тираж 10 000 экз.

Уважаемые читатели!

Издательство "Русская Редакция" выпускает книги компьютерной тематики по актуальным версиям популярных программных продуктов. Мы переводим на русский язык бестселлеры ведущих издательств мира, а также сотрудничаем с авторитетными российскими авторами. Книги "Русской Редакции" рассчитаны на самый широкий круг читателей: от начинающих работать на компьютере до профессионалов.

Книги "Русской Редакции" Вы можете приобрести:

в Москве:

«Московский Дом Книги»

ул. Новый Арбат, 6

«Библио-Глобус»

ул. Мясницкая, 6

«Дом Технической книги»

Ленинский пр., 40

«Мир»

Ленинградский пр., 78

«Молодая гвардия»

(отдел АО «Кладезь»)

ул. Большая Полянка, 28

Торговый дом «Москва»

ул. Тверская, 8

ТОО «Алекс и К°»

Магазин «Книги»

г. Зеленоград, 1106^б

«Мульти-Пульти»

ул. Автозаводская, 5

в других городах:

г. Санкт-Петербург

ЗАО «Диалект»

(812) 534-4578

г. Новосибирск

ГПНТБ СОРАН

(3832) 66-8567

г. Тольятти

«АвтоВАЗВостокСервис»

(8469) 39-0248

Украина, г. Киев

Фирма «Евроиндекс Лтд.»

(044) 441-2512

Республика Беларусь, г. Минск

ЧП Никулин А. В.

(0172) 20-9571

Республика Казахстан,

г. Караганда

МП «Орман»

(3212) 58-0922

Книги нашего издательства Вы можете заказать по почте

АО «Аскери» тел. (095) 917-7289

ЛУЧШАЯ КОМПЬЮТЕРНАЯ ЛИТЕРАТУРА



Издательство «Русская Редакция» готовит к выпуску

Бестселлер 1996 г.

Билл Гейтс «Дорога в будущее»

Описания популярных программных продуктов

Брюс МакКинней Крепкий орешек Microsoft® Visual Basic® 4

Дэвид Дж. Круглински Основы Microsoft® Visual C++™ 4

Хелен Кастер Основы Microsoft® Windows NT™ и Файловая система NTFS

Microsoft Press Компьютерные сети (рабочее название)

Рони Шушан, Дон Райт и Лора Льюис Дизайн и компьютер (рабочее название)

Подарочная серия «Путеводители»

Стефен Л. Нелсон Путеводитель по Microsoft® Windows® 95

Стефен Л. Нелсон Путеводитель по Internet

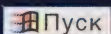
Авторские издания

Д. Хавжу и др. Макинтош для пользователя

Ф. Зубанов Windows NT™ — выбор «профи» (второе издание с учетом версии 4)

Г. Бугрименко, Е. Рыбкин Азбука 3D Studio





Вышли русские версии
Microsoft Windows® 95
и Office для Windows® 95

Негатив фиксирует
реальность,
но не отражает её.
Только
легальные версии
Windows 95 и Office 95
позволят Вам проявить себя
и гарантируют
позитивный результат.

Как проявить себя так, чтобы проявить себя?

Вы думаете об экономии, а, по сути, экономите на себе – на собственных возможностях и преимуществах. Пользуясь легальной версией Windows® 95 и Office 95, Вы можете в любой момент обратиться за помощью в Службу технической поддержки Microsoft. Вы можете использовать мощный интеллектуальный потенциал специалистов фирмы. Вам гарантированы скидки при покупке новых программных продуктов Microsoft. Принимая решение, помните: украсть программный продукт легко, службу технической поддержки украсть невозможно. Примите правильное решение – проявите себя!



Microsoft®

WHERE DO YOU WANT TO GO TODAY™

ВЕСТЬ АО — системный интегратор прикладных информационных систем в архитектуре "клиент-сервер" предлагает прикладные решения для различных областей деятельности на базе Microsoft Windows NT:

Microsoft
SOLUTION PROVIDER

Microsoft
AUTHORIZED DEALER

- корпоративная система управления документами и заданиями. Включает модули маршрутизации и контроля исполнения заданий — WorkRoute и модуль для работы с изображениями бумажных документов DeltaImage;
- система автоматизации торговой деятельности "Экипаж";
- система электронной разработки и хранения чертежно-конструкторской документации TechnoDOCS.

Техническая поддержка

ВЕСТЬ АО обеспечивает техническую поддержку по всем продуктам семейства BackOffice.

Тел. (095) 115-6001

Обучение

Microsoft
AUTHORIZED TRAINING CENTER

Учебный центр ВЕСТЬ АО (имеет статус Microsoft Authorized Training Center) проводит обучение для администраторов сетей и пользователей по продуктам Microsoft, в том числе по Windows NT:

Supporting Microsoft Windows NT

5-дневный курс для администраторов сетей, настраивающих и сопровождающих Microsoft Windows NT

Supporting Microsoft Windows NT Server

5-дневный курс для администраторов сетей, устанавливающих и сопровождающих Microsoft Windows NT Server

Accelerated Training for Microsoft Windows NT

5-дневный ускоренный курс для администраторов сетей, устанавливающих и сопровождающих Microsoft Windows NT Workstation и Server

После окончания курсов в Учебном центре ВЕСТЬ АО и сдачи сертификационных экзаменов выдаются сертификаты Microsoft Certified Product Specialist и Microsoft Certified Systems Engineer.

Занятия проводятся по программам и учебным пособиям, полученным непосредственно от Microsoft.

Преподаватели учебного центра имеют квалификацию Microsoft Product Specialist, Microsoft Certified Trainer, Microsoft Systems Engineer.

КОМПАНИЯ
ВЕСТЬ

ВЕСТЬ АО: тел: +7(095)115-6001; факс: +7(095)112-2333; e-mail: postmaster@vest.msk.ru
<http://www.vest.msk.ru>



наш подписной индекс 50247

<http://www.ritmpress.ru>, <http://www.relis.ru>

ВАШ ХОД



СЕТЕВАЯ АКАДЕМИЯ

Обучение сетям — из первых рук

Подготовка
Сертифицированных
Специалистов
по Windows NT

Microsoft
AUTHORIZED TRAINING CENTER

107066 Москва, Доброслѣбодская, 5
Тел.: (095) 267-3038, факс: (095) 265-5101
E-mail: academy@lanit.msk.su
<http://www.academy.lanit.msk.su>





МЫ И ТЫ

ВЫБОР — ПРОФ И

Федор
Зубанов